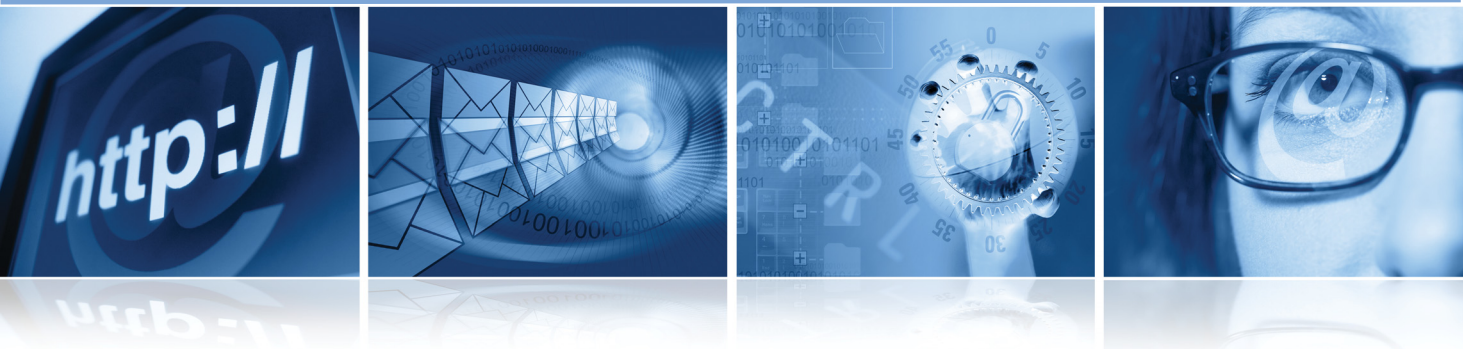


SECURE
COMPUTING®



ADMINISTRATION GUIDE

SnapGear Network Gateway Security

Version 3.1.5

SECURE COMPUTING®

SnapGear®
Network Gateway Security

www.securecomputing.com

Copyright

© 2007 Secure Computing Corporation. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Secure Computing Corporation.

Trademarks

Secure Computing, SafeWord, Sidewinder, Sidewinder G2, Sidewinder G2 Firewall, SmartFilter, Type Enforcement, CipherTrust, IronMail, IronIM, Softoken, Enterprise Strong, Mobile Pass, G2 Firewall, PremierAccess, SecureSupport, SecureOS, Bess, Cyberguard, SnapGear, Total Stream Protection, Webwasher, Strikeback and Web Inspector are trademarks of Secure Computing Corporation, registered in the U.S. Patent and Trademark Office and in other countries. G2 Enterprise Manager, SmartReporter, SecurityReporter, Application Defenses, Central Management Control, RemoteAccess, SecureWire, TrustedSource, On-Box, Securing connections between people, applications and networks and Access Begins with Identity are trademarks of Secure Computing Corporation.

Software License Agreement

CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE LOADING THE SOFTWARE. THIS AGREEMENT GOVERNS THE USE OF THE SOFTWARE (AS DEFINED BELOW). BY CLICKING "I ACCEPT" BELOW, OR BY INSTALLING, COPYING, OR OTHERWISE USING THE SOFTWARE, YOU ARE SIGNING THIS AGREEMENT, THEREBY BECOMING BOUND BY ITS TERMS. BY INDICATING YOUR AGREEMENT, YOU ALSO REPRESENT AND WARRANT THAT YOU ARE A DULY AUTHORIZED REPRESENTATIVE OF THE ENTITY THAT HAS PURCHASED THE SOFTWARE AND THAT YOU HAVE THE RIGHT AND AUTHORITY TO ENTER INTO THIS AGREEMENT ON THE ENTITY'S BEHALF. IF YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT, THEN CLICK "I DO NOT ACCEPT" BELOW OR DO NOT USE THE SOFTWARE AND RETURN ALL COPIES OF THE SOFTWARE, ASSOCIATED HARDWARE AND DOCUMENTATION TO SECURE COMPUTING CORPORATION ("SECURE COMPUTING") OR THE RESELLER FROM WHOM YOU OBTAINED THE SOFTWARE.

1. SOFTWARE PRODUCTS DEFINITION. "Software Product(s)" means (i) the machine-readable object-code versions of the SnapGear software that has been pre-loaded onto the SnapGear appliance (the "Software"), (ii) the published user manuals and documentation that are made available for the Software (the "Documentation"), and (iii) any updates or revisions of the Software or Documentation that you may receive (the "Update"). Under no circumstances will you receive any proprietary source code of the Software.

2. GRANT OF LICENSE. Secure Computing grants to you, and you accept, a non-exclusive, and non-transferable license (without right to sub-license) to use the Software Product as defined herein solely on and in conjunction with the Secure Computing appliance on which the Software is installed.

3. LIMITATION OF USE. You may not: 1) copy, except to make one copy of the Software solely for back-up or archival purposes; 2) transfer, distribute, rent, lease or sublicense all or any portion of the Software Product to any third party; 3) translate, modify, adapt, decompile, disassemble, or reverse engineer any Software Product in whole or in part; or 4) modify or prepare derivative works of the Software Products. You agree to keep confidential and use your best efforts to prevent and protect the contents of the Software Product from unauthorized disclosure or use. Secure Computing reserves all rights that are not expressly granted to you.

4. DISCLAIMER OF WARRANTIES. Secure Computing does not warrant that the functions contained in the Software Product will meet your requirements or that operation of the program will be uninterrupted or error-free. The entire risk as to the results and performance of the Software Product is assumed by you. THE SOFTWARE PRODUCT IS FURNISHED, "AS IS" WITHOUT ANY WARRANTY OF ANY KIND, AND SECURE COMPUTING AND ITS LICENSORS HEREBY DISCLAIM ALL WARRANTIES, EXPRESS, IMPLIED OR STATUTORY IN RESPECT OF THE SOFTWARE PRODUCT INCLUDING, WITHOUT LIMITATION, ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES AS TO NON-INFRINGEMENT. SOME STATES AND COUNTRIES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS WHICH VARY BY STATE OR COUNTRY.

5. LIMITATION OF REMEDIES. THE ENTIRE LIABILITY OF SECURE COMPUTING AND ITS LICENSORS UNDER, FOR BREACH OF, OR ARISING OUT OF THIS AGREEMENT, IS LIMITED TO A REFUND OF THE PURCHASE PRICE OF THE PRODUCT OR SERVICE THAT GAVE RISE TO THE CLAIM. IN NO EVENT SHALL SECURE COMPUTING OR ITS LICENSORS BE LIABLE FOR YOUR COST OF PROCURING SUBSTITUTE GOODS. IN NO EVENT WILL SECURE COMPUTING OR ITS LICENSORS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL, EXEMPLARY, OR OTHER DAMAGES WHETHER OR NOT SECURE COMPUTING HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

6. **TERM AND TERMINATION.** This license is effective until terminated. You may terminate it at any time by destroying the Software Product, including all computer programs and documentation, and erasing any copies residing on computer equipment. This Agreement also will automatically terminate if you do not comply with any terms or conditions of this Agreement. Upon such termination you agree to destroy the Software Product and erase all copies residing on computer equipment.

7. **PROTECTION OF CONFIDENTIAL INFORMATION.** The Software Product is delivered to you on a confidential basis and you are responsible for employing reasonable measures to prevent the unauthorized disclosure or use thereof, which measures shall not be less than those measures employed by you in protecting your own proprietary information. You may disclose the Software Product to your employees as necessary for the use permitted under this Agreement. You shall not remove any trademark, trade name, copyright notice or other proprietary notice from the Software Product.

8. **OWNERSHIP.** This Software is licensed (not sold) to you. All intellectual property rights including trademarks, service marks, patents, copyrights, trade secrets, and other proprietary rights in or related to the Software Products are and will remain the property of Secure Computing or its licensors, whether or not specifically recognized or protected under local law, provided however that certain components of the Software are components licensed under the GNU General Public License (version 2), which Secure Computing supports. You may obtain a copy of the GNU General Public License at <http://www.fsf.org/copyleft/gpl.html>. Secure Computing will provide source code for any of the components of the Software licensed under the GNU General Public License upon request. You will not remove any product identification, copyright notices, or other legends set forth on the Software Product.

9. **EXPORT RESTRICTIONS.** You agree to comply with all applicable United States export control laws, and regulations, as from time to time amended, including without limitation, the laws and regulations administered by the United States Department of Commerce and the United States Department of State. You have been advised that Software Products are subject to the U.S. Export Administration Regulations. You shall not export, import or transfer Software Products contrary to U.S. or other applicable laws, whether directly or indirectly, and will not cause, approve or otherwise facilitate others such as agents or any third parties in doing so. You represent and agree that neither the United States Bureau of Export Administration nor any other federal agency has suspended, revoked or denied your export privileges. You agree not to use or transfer the Products for end use relating to any nuclear, chemical or biological weapons, or missile technology unless authorized by the U.S. Government by regulation or specific license.

10. **U.S. GOVERNMENT RIGHTS.** Any Software or Documentation acquired by or on behalf of a unit or agency of the United States Government is "commercial computer software" or "commercial computer software documentation" and, absent a written agreement to the contrary, the Government's rights with respect to such Software or Documentation are limited by the terms of this Agreement, pursuant to FAR § 12.212(a) and its successor regulations and/or DFARS § 227.7202-1(a) and its successor regulations, as applicable.

11. **ENTIRE AGREEMENT.** This Agreement is our offer to license the Software Product to you exclusively on the terms set forth in this Agreement, and is subject to the condition that you accept these terms in their entirety. If you have submitted (or hereafter submit) different, additional, or other alternative terms to Secure Computing or any reseller or authorized dealer, whether through a purchase order or otherwise, we object to and reject those terms. Without limiting the generality of the foregoing, to the extent that you have submitted a purchase order for the Software Product, any shipment to you of the Software Product is not an acceptance of your purchase order, but rather is a counteroffer subject to your acceptance of this Agreement without any objections or modifications by you. To the extent that we are deemed to have formed a contract with you related to the Software Product prior to your acceptance of this Agreement, this Agreement shall govern and shall be deemed to be a modification of any prior terms in their entirety.

12. **GENERAL.** Any waiver of or modification to the terms of this Agreement will not be effective unless executed in writing and signed by Secure Computing. If any provision of this Agreement is held to be unenforceable, in whole or in part, such holding shall not affect the validity of the other provisions of this Agreement. You may not assign this License or any associated transactions without the written consent of Secure Computing. This License shall be governed by and construed in accordance with the laws of California, without regard to its conflicts of laws provisions.

Customer Advocate information

To suggest enhancements in a product or service, or to request assistance in resolving a problem, please contact a Customer Advocate at +1.877.851.9080. If you prefer, send an e-mail to customer_advocate@securecomputing.com.

If you have comments or suggestions you would like to make regarding this document or any other Secure Computing document, please send an e-mail to techpubs@securecomputing.com.

Publishing history

Date	Part number	Firmware release
July 2007	86-0946754-A	3.1.5u1

CONTENTS

	Preface	xi
	Welcome	xi
	Who should read this guide	xi
	Where to find additional information	xi
	Typographical conventions	xii
CHAPTER 1	Introduction	1
	SnapGear gateway appliances (SG300, SG5xx series)	2
	Front panel LEDs	3
	Rear panel	6
	Physical specifications	6
	SnapGear rack mount appliance (SG720)	7
	Front panel LEDs	7
	Front panel	8
	Rear panel	8
	Physical specifications	8
	SnapGear PCI appliance (SG640)	9
	Bridged mode	9
	LEDs	10
	Physical specifications	10
	SnapGear Management Console	11
	Welcome page	11
	Product registration links	12
	My SnapGear login page	13
	SnapGear menus	19
	Interface icons	24
	Online help icon	24
	Backup and restore icon	24
	Edit and delete icons	24
	Add above and below icons	25
	Tooltips	25
	Help and Support menu option	26
	Online Help page	26
	Technical Support page	27
	Technical Support Report page	28
	SnapGear Portal	29

	Solution Finder	31
CHAPTER 2	Network Setup Menu Features	33
	Network setup overview	34
	Multifunction vs. fixed-function ports	34
	Direct Connection Settings page	38
	Ethernet Configuration tab	40
	Aliases tab	43
	Enabling IPv6 for a connection	44
	Routed versus bridged DSL modems	46
	Connecting with a cable modem	55
	Configuring dialout port settings	61
	Configuring static IP addresses for a connection	64
	Configuring interface aliases for a connection	65
	Dial-in setup	66
	Failover, load balancing, and high availability	75
	Internet connection failover	77
	Editing failover connection parameters	77
	Modifying failover levels	81
	High Availability	86
	DMZ network	94
	Services on the DMZ network	96
	Wireless	99
	Wireless security methods	99
	Configuring a wireless connection	100
	Configuring Wireless MAC-based ACL	110
	Bridging	119
	Adding a bridged interface	119
	Deleting a bridge	126
	Bridging across a VPN connection	126
	VLAN	127
	Adding a VLAN	127
	Port-Based VLANs	129
	Enabling port-based VLANs	130
	Troubleshooting GRE tunnels	138
	Routes	139
	Creating a static route	139
	Enabling route management	143
	Example: Configuring RIP Route Management	144
	Example: OSPF	146
	Entering device settings	151
	DNS	153
	DNS Proxy tab	153
	DHCP Server	162
	DHCP Addresses page	167
	DHCP Relay page	171

Web cache	176
Creating a user account and network share in Windows XP	178
Allocating network storage for Web cache	180
Configuring ICAP client for Web Cache	186
Configuring advanced settings for the Web cache	187
QoS Traffic Shaping	190
Enabling QoS Autosshaper	190
IPv6 tab	196
Enabling IPv6 at the appliance level	196
SIP Proxy tab	198
Enabling the SIP proxy	199

CHAPTER 3

Firewall menu	201
Administration Services page	204
Packet filtering	231
Custom Firewall Rules tab	242
NAT	245
About port forwarding	245
Source NAT page	257
Connection tracking	274
Configuring connection tracking	276
Benefits of using an IDS	284
Configuring basic IDB	285
Advanced Intrusion Detection and Prevention	292
Configuring Snort in IPS mode	293
Configuring Snort in IDS mode	294
Setting up the analysis server for Snort IDS	296
Access control	297
ACL tab	304
Web Lists tab	307
Policy enforcement	310
Uploading a Webwasher certificate and key	321
Copying and pasting a Webwasher certificate and key	322
Virus scanning Web traffic	337
Antispam (TrustedSource)	340
About TrustedSource	340
Enabling TrustedSource	342

CHAPTER 4

VPN	347
About VPN	348
About PPTP	349
PPTP VPN Client	349
PPTP VPN Server	352
Enabling and configuring the PPTP VPN Server	353
Adding a PPTP user account	355
Setting up a Windows XP PPTP client	356

L2TP VPN Server	363
Configuring the L2TP VPN server	363
About IPsec VPN	376
Enabling IPsec VPN	378
IPsec status details overview	384
Keying modes	387
Setting up a tunnel with RSA signatures authentication	394
Aggressive keying mode for an IPsec tunnel	401
Converting an IPsec tunnel configuration to the advanced format ..	408
IPsec example	410
SnapGear appliance to SnapGear appliance	410
Setting up the branch office	410
NAT traversal support	419
Dynamic DNS support	419
Certificate management	420
The OpenSSL application	420
Extracting a PKCS12 certificate	420
Creating a self-signed certificate	421
Adding a certificate for use with IPsec VPN	431
IPsec failover	435
IPsec VPN offloading	444
Troubleshooting IPsec	447
IPsec tips	447
IPsec symptoms, causes, and solutions	447
Configuring an HTTP tunnel server	455
Configuring an SSL tunnel server	458
Creating nested port tunnels	460

CHAPTER 5

System menu features	461
Date and Time menu	462
Setting locality	463
Syncing appliance date and time with a PC	464
Enabling the NTP time server	465
Adding an NTP server	468
Adding an NTP peer	468
Backup/Restore menu	469
Remote Backup/Restore page	470
Local Backup/Restore page	472
Text save/restore tab	474
Users menu	476
Administrative users page	476
PCI DSS page	479
Adding a local user	480
RADIUS page	483
TACACS+ page	485
Management menu	486

	Configuring CommandCenter management	486
	Enabling CommandCenter Debug Logging	488
	CMS Attributes	493
	Enabling the SNMP agent	495
	Diagnostics menu	497
	System tab	497
	Viewing the Local System Log	498
	Configuring local system log settings	499
	Enabling remote system logging	501
	Network Tests page	503
	Detected USB Devices	505
	Packet Capture page	506
	Advanced menu	511
	Reboot and Reset	511
	Soft rebooting the device	511
	Halting the appliance before powering down	512
	Erasing configuration and rebooting	512
	Upgrading firmware	513
	Upgrading flash firmware via HTTP	514
	Upgrading flash firmware via TFTP	516
	Configuration Files tab	519
CHAPTER 6	USB	523
	USB mass storage devices	524
	Sharing a USB storage device	525
	Joining a Windows workgroup	528
	Example: Partitioning a USB storage device	529
	USB printers	532
	Setting up a shared USB printer	532
	Setting up a printing spool	534
	Setting up a Windows PC for remote printing	536
	Troubleshooting printing	540
	Print driver installation fails	541
	Printer appears in Printers and Faxes, but printing still fails	541
	Printing still fails	542
	LPR/LPD	542
APPENDIX A	System Log	543
	Access logging	544
	Creating custom log rules	546
	Rate limiting	548
	Administrative access log messages	549
	Boot log messages	549
APPENDIX B	Upgrading firmware	551
	Firmware upgrade best practices and precautions	552

	Restoring factory default settings	553
	Upgrading firmware using Netflash	553
	Recovering from a failed upgrade	554
	Recovery using Netflash	554
	Recovery using a BOOTP server	556
APPENDIX C	Null modem administration	559
	Null modem	560
	Enabling null modem dial-in	560
	Enabling null modem dial out of the local PC	560
	Troubleshooting	561
APPENDIX D	CLI commands	563
	Programs and commands	564
APPENDIX E	Downloading antivirus database files.	579
	Downloading and configuring clam database files	580
	Index	589

PREFACE

Welcome

This guide describes the features and capabilities of your SnapGear appliance, and provides you with instructions on how to best take advantage of them. The document organization follows the menu layout of the SnapGear graphical user interface, with the exception of the USB chapter. The Appendices contain additional information for maintenance and reference information.

Who should read this guide

You should read this guide if you are responsible for evaluating, installing, operation, or managing a SnapGear appliance. This guide assumes you are familiar with the internal network of your organization. You should also have some knowledge of the Internet, HTTP (Hypertext Transfer Protocol), and FTP (File Transfer Protocol).

Where to find additional information

The following table contains related documentation and additional sources of information.

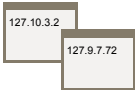
Table 1: Related documentation

Document	Description
SnapGear <i>Quick Install Guide</i>	Leads you through your initial SnapGear configuration.
Online help	Online help is available SnapGear for each page and its corresponding fields. For more information about the help system, see “Help and Support menu option” on page 26.
Knowledgebase	The SnapGear portal contains a knowledgebase for technical how-to articles, access to free Web-based training, and a solution finder for featured configuration options such as VPN, and packet filter and NAT rules. For more information, see “SnapGear Portal” on page 29. The SnapGear portal is available at the following URL: http://sgkb.securecomputing.com

Typographical conventions

This guide uses the following typographical and document conventions:

Table 2: Conventions used in this guide

Convention	Description
boldface courier	Commands and keywords you type at a system prompt are in boldface courier font.
<code>\</code> (backslash character in a command string)	When a command does not fit on the same line in this document, the backslash (\) character is used to indicate continuation. Enter the command as shown, ignoring the backslash.
<i>courier italic</i>	Placeholders for text you type. Words that appear in angle brackets <xxx> are placeholders for optional text.
<code>courier plain</code>	Text displayed by this product on a computer screen.
<i>plain text italics</i>	Names of files and directories; references to other documentation sources.
Body Text Highlight	Buttons, field names, and tabs in procedures that require user interaction.
<u>Note:</u>	Reader take note. Notes contain helpful suggestions or references to material not covered elsewhere in the manual.
<u>Tip:</u>	The information within describes a time-saving action or might help you solve a problem.
<u>Important:</u>	The text within provides information essential to the successful completion of a task or procedure.
<u>Caution:</u>	Instructs the reader to exercise caution. In this situation, you might do something that could result in loss of data or an unpredictable outcome.
<u>Security Alert:</u>	Emphasizes information that is critical to maintaining product integrity or security.
127.10.3.4 	IP addresses, screen captures, and graphics within this document are intended as examples. They do not necessarily represent a proper or complete configuration or the configuration that is appropriate to your needs. Often features are enabled so they are clear in the screen capture. Not all features are appropriate or desirable for your SnapGear setup.



CHAPTER 1

Introduction

In this chapter...

SnapGear gateway appliances (SG300, SG5xx series)	2
SnapGear rack mount appliance (SG720)	7
SnapGear PCI appliance (SG640)	9
SnapGear Management Console	11
SnapGear menus	19
Interface icons	24
Help and Support menu option	26
SnapGear Portal	29

SnapGear gateway appliances (SG300, SG5xx series)

Note: The SG gateway appliance range includes models SG300, SG560, SG565, and SG580.

The SnapGear gateway appliance range provides Internet security and privacy of communications for small and medium enterprises, and branch offices. It simply and securely connects your office to the Internet, and with its robust stateful firewall, shields your computers from external threats.

By default, all SnapGear appliances run a fully secured stateful firewall. This means from the PC (Personal Computer) that the appliance is plugged into, most network resources are freely accessible. However, any services that the PC provides, such as file shares or Web services such as IIS are *not* accessible by other hosts on the internet without further configuration of the SnapGear appliance. This is accomplished using packet filter rules. For details, refer to “Packet filtering” on page 231.

With the SnapGear appliance's masquerading firewall, hosts on your LAN (Local Area Network) can see and access resources on the Internet, but all that outsiders see is the SnapGear appliance's external address.

You can tailor your appliance to disallow access from your LAN to specific Internet sites or categories of content, give priority to specific types of network traffic, and allow controlled access to your LAN from the outside world. You can also choose to enable intrusion detection and prevention services on your SnapGear appliance, to further bolster the security of your local network.

The SG560, SG565, and SG580 can also connect to a DMZ (DeMilitarized Zone) network. A DMZ is a separate local network typically used to host servers accessible to the outside world. It is separated both physically and by the firewall, in order to shield your LAN from external traffic.

The SnapGear appliance allows you to establish a VPN (Virtual Private Network). A VPN enables remote workers or branch offices to connect securely to your LAN over the public Internet. The SnapGear appliance can also connect to external VPNs as a client. The SG560, SG565, and SG580 use onboard cryptographic acceleration to ensure excellent VPN throughput.

You can configure the appliance with multiple Internet connections. These auxiliary connections can be kept on standby should the primary connection become unavailable, or maintained concurrently with the primary connection for spreading network load.

The SG565 and SG580 incorporate a powerful Web proxy cache to improve Web page response time and reduce link loads. It is designed to integrate seamlessly with upstream proxy caches provided by ISPs.

Front panel LEDs

The front and rear panels contain LEDs indicating status. LEDs and labels vary from model to model. The labels for the front panel LEDs are detailed in the following tables.



Important: If H/B does not begin flashing shortly after power is supplied, refer to “Recovering from a failed upgrade” on page 554.

Table 3: SG300 LED descriptions

Label	Activity	Description
Power	On (steady)	Power is supplied to the SnapGear appliance.
TST	Flashing	Similar to H/B light on other models. The appliance is operating correctly.
	On	If this LED is on and not flashing, an operating error has occurred.
	Off	If the power is on and the H/B light is off, either the Halt Now option is activated in preparation to power down safely, or an operating error has occurred.
LAN1, LAN2, LAN3, LAN4	Flashing	Indicates network traffic on the LAN network interfaces.
WAN	Flashing	Indicates network traffic on the Internet network interface.

Table 4: SG560and SG580 LED descriptions

Label	Activity	Description
Power	On (steady)	Power is supplied to the SnapGear appliance.
H/B (Heart Beat)	Flashing steadily	The appliance is operating correctly.
	On	If this LED is on and not flashing, an operating error has occurred.
	Off	If the power is on and the H/B light is off, either the Halt Now option is activated in preparation to power down safely, or an operating error has occurred.
ETH A	Flashing	Indicates activity on the 4 port switch.
ETH B	Flashing	Indicates activity on Port B.
Serial	Flashing	Indicates the COM port is receiving and transmitting data.
HA	On	High Availability. The appliance has switched to a backup device.
Online	On (steady)	An Internet connection has been established.
VPN	On	Virtual private networking is active.

Table 5: SG565 LED descriptions

Label	Activity	Description
Power	On (steady)	Power is supplied to the SnapGear appliance.
H/B (Heart Beat)	Flashing steadily	The appliance is operating correctly.
	On	If this LED is on and not flashing, an operating error has occurred.
	Off	If the power is on and the H/B light is off, either the Halt Now option is activated in preparation to power down safely, or an operating error has occurred.
ETH	Flashing	Indicates network traffic.
USB	Flashing	Indicates activity on an attached USB device.
WLAN	Flashing	Indicates network traffic on the Wireless network interface.
Serial	Flashing	Indicates the COM port is receiving and transmitting data.
Online	On (steady)	An Internet connection has been established.
VPN	On	Indicates Virtual Private Networking is active. If IPsec tunnels are configured, the light illuminates when a valid IPsec tunnel is active. If there are no IPsec tunnels configured, the LED illuminates for the PPTP VPN Server. For the VPN LED, IPsec takes precedence over other VPN configurations. For further information on VPN, see Chapter 4.

Rear panel

The rear panel contains Ethernet and serial ports, the erase button, and power inlet. The serial port can be connected to an analog/ISDN modem or terminal for serial console access.

Note: For instructions on serial console access, refer to Appendix C, Null modem administration.

If network status LEDs are present for the ports (not present on the SG300 model), the lower or left LED indicates the link condition, where a cable is connected correctly to another device. The upper or right LED indicates network activity.

Physical specifications

The following are the local or wide area network link specifications:

- 10/100BaseT 4 port LAN switch (SG300)
- 10/100BaseT 4 port VLAN-capable switch (SG560, SG565, SG580)¹
- Serial (for dial-up/ISDN)
- Front panel serial status LEDs (for TX/RX)
- Online status LEDs (for Internet/VPN)
- Rear panel Ethernet link and activity status LEDs

The following are the environmental specifications:

- External power adaptor (voltage/current depends on individual model)
- Front panel operating status LEDs: Power, H/B
- Operating temperature between 0° C and 40° C
- Storage temperature between -20° C and 70° C
- Humidity between 0 to 95% (non-condensing)

1. Port A1 is set to LAN and cannot be changed.

SnapGear rack mount appliance (SG720)

The SG720 is the flagship of the SnapGear appliances. It features multi-megabit throughput, rack-optimized form factor, three fast Ethernet ports, and two gigabit ports. There are no switches on the SG720; all ports are bona fide ports.

In addition to providing all of the features described in the Gateway Appliances models, the SG720 model equips central sites to securely connect hundreds of mobile employees and branch offices.

Front panel LEDs

The front panel contains LEDs indicating status. On the front panel Ethernet ports, the orange LED on the upper right indicates the link condition when a cable is connected correctly to another device. The flashing green LED to the upper left indicates network activity. A description of the front panel LEDs are detailed in the following table.



Important: If H/B does not begin flashing shortly after power is supplied, refer to “Recovering from a failed upgrade” on page 554.

Table 6: SG7xx LED descriptions

Label	Activity	Description
Online	On	An Internet connection has been established.
Failover	On	The appliance has switched to the backup Internet connection.
PWR	On	Power is supplied to the SnapGear appliance.
H/B (Heart Beat)	Flashing	The appliance is operating correctly.
	On	If this LED is on and not flashing, an operating error has occurred.
	Off	If the power is on and the H/B light is off, either the Halt Now option is activated in preparation to power down safely, or an operating error has occurred.
High Avail	On	High Availability. Indicates the appliance has switched to a backup appliance.

Front panel

The front panel contains two 10/100/1000 GbE (Gigabit Ethernet) ports (A and B), three 10/100BaseT FE (Fast Ethernet) ports (C, D, and E), a serial port that can be connected to an analog/ISDN modem or terminal for serial console access, as well as operating status LEDs and the configuration erase button.

Note: For instructions on serial console access, refer to Appendix C, Null modem administration.

Rear panel

The rear panel contains a power switch and a power inlet for an IEC power cable.

Physical specifications

The following are the connectivity specifications:

- Two 10/100/1000 GbE ports (A¹ and B)
- Three 10/100BaseT FE ports (C, D, E)
- Serial port
- Online status LEDs (Online, Failover, High Availability)
- Ethernet link and activity status LEDs

The following are the environmental specifications:

- Front panel operating status LEDs: Power, H/B
- Operating temperature between 0° C and 40° C
- Storage temperature between -20° C and 70° C
- Humidity between 0 to 95% (non-condensing)

1. Port A is set to LAN and cannot be changed.

SnapGear PCI appliance (SG640)

The SG PCI appliance is a hardware-based firewall and VPN server embedded in a 10/100 Ethernet PCI network interface card (NIC). It is installed into the host PC like a regular NIC, providing a transparent firewall to shield the host PC from malicious Internet traffic, and VPN services to allow secure remote access to the host PC.

Unlike other SnapGear gateway and rack mount appliances, a single SnapGear PCI appliance is not intended as a means for your entire office LAN to be connected to, and shielded from, the Internet. Installing a SnapGear PCI appliance in each network-connected PC gives it its own independently manageable, enterprise-grade VPN server and firewall, running in isolation from the host operating system. This approach offers an increased measure of protection against internal threats as well as conventional Internet security concerns. You can update, configure and monitor the firewall and VPN connectivity of a workstation or server from any Web browser. In the event of a breach, you have complete control over access to the host PC independently of its operating system, even if the host PC has been subverted and is denying normal administrator access.

All network filtering is handled entirely by the SnapGear appliance. This has the advantage over the traditional approach of using a host-based personal software firewall and VPN service by not taxing the host PC's resources.

Bridged mode

By default, the PCI appliance operates in bridged mode. This is distinctly different from the masquerading behavior of SnapGear gateway and rack mount appliances.

In bridged mode, the PCI appliance uses two IP addresses. Note that these addresses are both in the same subnet as the LAN, as no masquerading is being performed.

Note: *It is possible to configure the SG PCI appliance to run in masquerading mode. For more information, refer to "Masquerading page" on page 268.*

One IP address is used to manage the SnapGear appliance via the Web management console. The other is the host PC's IP address, which is configurable through the host operating system, identically to a regular NIC. This is the IP address that other PCs on the LAN see. It should be dynamically (DHCP) or statically configured to use the same gateway and DNS settings as a regular PC on the LAN.

LEDs

The rear panel contains LEDs indicating status. The two LEDs closest to the network port are network activity (upper) and network link (lower). The two other LEDs are power (upper) and heart beat (lower).

Table 7: SG6xx LED descriptions

Location	Activity	Descriptions
Top right (Power)	On	Power is supplied to the appliance.
Bottom right (Heart beat)	Flashing	The appliance is operating correctly.
	On	If this LED is on and not flashing, an operating error has occurred.
	Off	If the power is on and the H/B light is off, either the Halt Now option is activated in preparation to power down safely, or an operating error has occurred.
Top left (Network activity)	Flashing	Data is being transmitted or received.
Bottom left (Network link)	On	The appliance is attached to the network.

Note: If the Heart Beat does not begin flashing shortly after power is supplied, refer to “Recovering from a failed upgrade” on page 554.

Physical specifications

The following are the network link specifications:

- 10/100baseT Ethernet port
- Ethernet LEDs (link, activity)

The following are the environmental specifications:

- Status LEDs: Power, Heart Beat
- Operating temperature between 0° C and 40° C
- Storage temperature between -20° C and 70° C
- Humidity between 0 to 95% (non-condensing)

SnapGear Management Console

Figure 1: SnapGear console—Welcome page



Note: Advanced users can customize the appearance of the console and override the default HTML styles. Create the file **localstyle.css** in the **/etc/config/** directory with the styles you prefer.

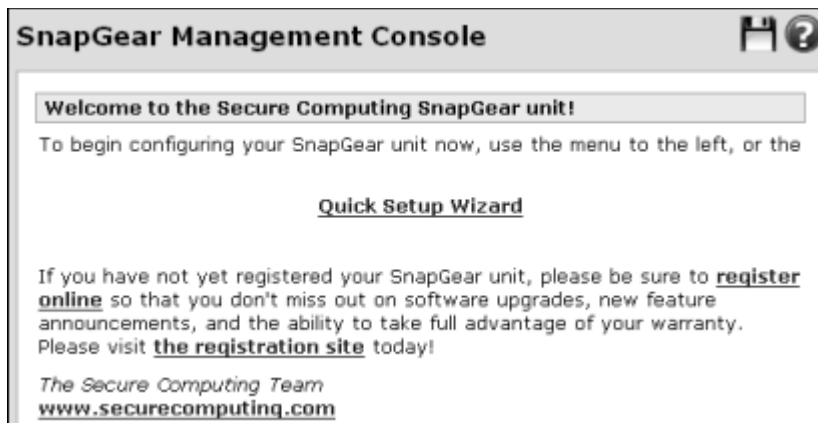
Welcome page

When you first establish connectivity with your SnapGear appliance, the Welcome page appears in the SnapGear Management Console. The Welcome page appears each time you first open a browser to your console. From the welcome page, you can access product registration links and the Quick Setup Wizard. You can click the product registration links either before or after completing the Quick Setup Wizard. For more information on the Quick Setup Wizard, refer to the *Quick Install Guide* for your appliance model. For more information on registering your product, see “Registering your SnapGear appliance” on page 15.

Product registration links

Register online to keep abreast of firmware updates and to take advantage of your warranty. The initial Welcome page contains links to the Quick Setup Wizard and product registration links.

Figure 2: Product registration links



My SnapGear login page

The URL for SnapGear product registration is:

<http://my.securecomputing.com>

A current email address is required to register your product. A password is emailed to you after you register. You can change your password once you log in. You also need to provide the serial number of your SnapGear appliance or appliances.

Figure 3: My SnapGear
Login page

Creating an account

- 1 If you need to create an account, click the **Click here if you need to create a new account** link. The My SnapGear New Account Request page appears.

Figure 4: My SnapGear
New Account Request
page

SECURE
COMPUTING

+1.800.379.4944 Toll Fr
+1.408.979.6572 International

log

My SnapGear™ New Account Request

Don't yet have a My SnapGear™ account?

Signing up is quick, easy, and free. Simply enter your e-mail address below and we will send you a custom url which may be used to gain access directly into the site. Once inside, you'll be able to change your password, register products or add-ons, update your support information, sign up for special product announcements, and access the latest firmware upgrades.

E-mail address:

- 2 Enter your **E-mail address** and click **Create Account**. A message indicates a new account request is currently being processed. Upon verification, a login password is e-mailed to you.

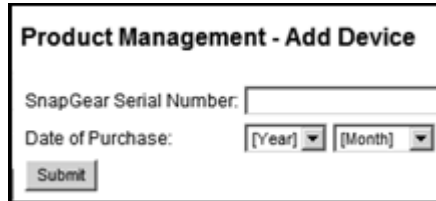
Once you log in, you can change your My SnapGear password, add products you own to your profile, download Beta firmware, and activate any add-on features you may have purchased.

Registering your SnapGear appliance

Use this procedure to add a product you have purchased to your My SnapGear profile.

- 1 Log in to the My SnapGear site at <http://my.securecomputing.com>.
- 2 Click **Add Products**. The Product Management - Add Device page appears.

Figure 5: My SnapGear Product Management — Add Device page



- 3 Enter the serial number of your SnapGear appliance in the **SnapGear Serial Number** field. The serial number is found on a sticker attached underneath the appliance.
- 4 Indicate the **Year** and **Month** for **Date of Purchase**.
- 5 Click **Submit**. To view a list of all product you have registered, click **List Products**.

Activating a feature

Use this procedure to activate an add on feature such as content filtering. Make sure you have registered your appliance and have the token provided to you for the feature.

- 1 Log in to the My SnapGear site at <http://my.securecomputing.com>.
- 2 Click **Activate Features**. The Product Management - Activate Feature page appears.

Figure 6: My SnapGear Product Management — Activate Feature page



Product Management - Activate Feature

SnapGear Serial Number: 0601860230330552 (SG565)

Feature Serial Number (token):

Submit

- 3 Select your SnapGear appliance from the **SnapGear Serial Number** list.
- 4 Enter the token in the **Feature Serial Number (token)** field.
- 5 Click **Submit**.

Retrieving license information for add-on products

Once you activate a feature, the license information becomes available to you. Click **View URL Filter License data**.

Figure 7: My SnapGear
Product Management -
License data

Product Management - Registered Devices			
Model	Serial Number / Location	Purchased	Options / Filtering
SG565	0601860230330552	2007-03-28	KIT, SG565 Webwasher 3 Month Trial Subscription View URL Filter License data

The certificate and private key are then displayed in text form.

Figure 8: My SnapGear Product Management - License data

```
Product Management - License Details

Please see this article for instructions on configuring your version of firmware for use
License (for firmware released prior to January 2006):

CFK0033M
(Note that this license may take up to 5 minutes from activation before it can be used.)

Certificate data (new firmware only):

-----BEGIN CERTIFICATE-----
MIIEOTCCA7mgAwIBAgICCFKwDQYJKoZIhvcNAQEFBQAwgbcxCzAJBgNVBAYTAkRF
MQwwCgYDVQQIEwN0U1cxEjAQBgNVBACTCVBhZGVyYm9yb2E5SMBAAG1UEChMjV2Vi
d2FzaGVyMR8wHQYDVQQLExZDYXR1Z29yaXphdG1vb1BTZXJ2aWN1MSwwKgYDVQDD
EYNXZWJ3YXNoZXIqQ2F0ZUdvcml6YXRpb24gU2VydmljZSB0QTEkMCIGCSqGSIb3
DQEJARYVc3VwcG9ydEB3ZWJ3YXNoZXIuY29tMB4XDzA3MDQwMzIxMDUxM1oXDzA3
MDUwMzIxMDUxM1owTELMMAkGA1UEBhMCREUxODAKBgNVBAgTA0VSSzEVEVBGALUE
ChMMd2ViZ2FzaGVyIEFHMwEQYDVQQLExpJVC1TZXJ2aWN1MSwwKgYDVQDDFCNj
PTMxODc0fGQ9MDYwMTg2MDIzMDMzMjU1MmxyPS0xZHU9MTcBnzANBgkqhkiG9w0B
AQEFAA0BJQAwwYkCgYEAxYzVpiVS1uQzCwCsIaxmVp8i3d6tpsEczRjQA/1VKKe5
A12NxoHj6fJDRdS1uDFqI23+17qoKYXjGCj0oMV+FYI8he2jF/RdDH2Fmhjg3Q
W0e0U0hw6S2/E7QvGgB84Pf13At7Cuk1b71FdxpTY0Y1DbvQy28hQIbgVUUCfUC
AwEAAa0CAakwggG1MAkGA1UdEwQCAAAwEQYJYIZIAYb4QgEBBAQDAgSwMCKGCUCG
SAGG+IEBQQcFhpTV01TIEdlbmVYXR1ZCBBDZXJ0aWZpY2F0ZTA3MDQwMzIxMDUx
R29vJ6cRlor120che6FqkkqW1bEwge0GA1UdIwSBSTCB4oAUYjxeLoYVFFUIB9RE
sqeTauqh10ehgb6kgbswgbgxCzAJBgNVBAYTAkRFMQwwCgYDVQQLExwN0U1cxEjAQ
BgNVBACTCVBhZGVyYm9yb2E5SMBAAG1UEChMjV2ViZ2FzaGVyMR8wHQYDVQQLExZD
YXR1Z29yaXphdG1vb1BTZXJ2aWN1MSwwKgYDVQDDQDEYNXZWJ3YXNoZXIuY29tMB4
cm16YXRpb24gU2VydmljZSB0QTEkMCIGCSqGSIb3DQEJARYVc3VwcG9ydEB3ZWJ3
YXNoZXIuY29tggkAuy6YD/eDfQEWcYDVROPAQDAgUgMD4GA1UdHwQ3MDUwM6Ax
oC+GLW0dHA6Ly93d3cuY311ZXJndWYyZC5jb20vcnV2b2t1bG1zqHmVY3JsLnB1
bTANBgkqhkiG9w0BAQUFAA0CAQEAEEZFuDxKb6q91NVom0J/WloXUx57Jnv2SKYeB
kTGuPK8GalfXapzA2x88Id5FFdkGZ1sPkeX67YjIq8cAKAhfcc3Rsm+abMDX5nFI
nN320Wcn0KmqQosfEUWZV1r71TYNIu8PTx8n9m1JBqri+ycqVYN0I2Y44uIfqUwDM
F885b990qmCcR659xT6sXMT8BqPg6EH1rqFEpUvLluephPpRC2iQFFHdj35qEUI
d216BmBjaloHsh0akk6sbesPBtknQJNEprKFmiV+WJvN9VI1Scx1UpRDpEpk2Fx9B
rsHMC8IGkGP9FD1Nn3ex19USaR0jktAG4LmoAtB/AbW2B3fimQ==
-----END CERTIFICATE-----

Key data (new firmware only):

-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQCtjNVm3VLW5DNLAKwhrGZWNyLd3q2awRzNEoD/VUOp7kCLY3G
```

You can then copy and paste the license key for Webwasher, for instance, into the Certificate copy/paste page.



Important: Be sure to include the ----Begin... and ----End... text lines in your copy and paste.

For further details, see “Uploading a Webwasher certificate and key” on page 321.

SnapGear menus

To navigate the interface, click the corresponding link in the menu. The menu options available depend on the particular model of a SnapGear appliance and the firmware version currently installed on the appliance.

Figure 9: SnapGear
Menus



An arrow and highlighting indicate your current menu selection. Connection Tracking is the currently selected menu option shown in Figure 9.

The SnapGear Web management console contains the following menus:

- Network Setup
- Firewall
- VPN
- System

The following tables give brief descriptions of the options available under each menu.

Table 8: Network Setup menu

Network Setup menu options	Description
Network Setup	<p>Opens the Connections, Failover & High Availability, Routes, System, DNS, and IPv6 tabs for configuring network-specific settings of the appliance.</p> <p>See:</p> <ul style="list-style-type: none"> • “Network setup overview” on page 34. • “Failover, load balancing, and high availability” on page 75. • “Routes” on page 139. • “System tab” on page 151. • “DNS” on page 153. • “IPv6 tab” on page 196.
DHCP Server	<p>Opens the DHCP Server Configuration page for handing out IP addresses. See “DHCP Server” on page 162.</p>
Web Cache	<p>Opens the Web Cache pages for caching pages on the SnapGear appliance. See “Web cache” on page 176.</p> <p>Note: <i>Not applicable to the SG300 or SG560 models.</i></p>
Shares	<p>Opens the Shares page for Storage and Printing. See Chapter 6, USB.</p> <p>Note: <i>Only applicable to the SG565 model.</i></p>
QoS Traffic Shaping	<p>Opens the Traffic Shaping pages for enabling and configuring QoS traffic. See “QoS Traffic Shaping” on page 190.</p>
SIP	<p>Opens the SIP Proxy page for enabling and configuration. See “SIP Proxy tab” on page 198.</p> <p>Note: <i>Not applicable to the SG300 model.</i></p>

Table 9: Firewall menu

Firewall menu options	Description
Incoming Access	Opens the Administration Services page, where you can configure the management of the appliance directly via telnet, SSH, web and SSL services. This page allows the control and restriction of access to these services from specific network interface types. See “Incoming access” on page 204.
Definitions	Opens the definitions pages for Service Groups, Addresses, and Interfaces. See “Definitions” on page 219.
Packet Filtering	Opens the Packet Filter Rules, Custom Firewall Rules, and Custom IPv6 Firewall Rules. See “Packet filtering” on page 231.
NAT	Opens NAT pages for Port Forwarding, Source NAT, 1 to 1 NAT, Masquerading, and UPnP Gateway. See “NAT” on page 245.
Connection Tracking	Opens the Connection Tracking page in which you can enable or disable specific options for connection tracking. Connection tracking keeps a record of packets that have passed through the appliance and how the packets are interrelated. See “Connection tracking” on page 274.
Intrusion Detection	Opens the configuration pages for Intrusion Detection and Prevention. See “Intrusion Detection Systems” on page 284. <i>Note: Snort IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) features are not applicable to the SG300 or SG560 models. Basic IDB (Intrusion Detection and Blocking) is available on all SnapGear models.</i>
Access Control	Opens the Authorizations pages for Access Control, ACL, Web Lists, Policy, Webwasher, and legacy content filtering. See “Access control” on page 297.
Antivirus	Opens the Antivirus pages where you can configure antivirus for Email, Web downloads, and FTP. See “Antivirus” on page 327. <i>Note: Not applicable to the SG300 or SG560 models.</i>
Antispam	Opens the TrustedSource page for configuring reputation thresholds for SMTP mail. See “Antispam (TrustedSource)” on page 340.

Table 10: VPN menu

VPN menu options	Description
PPTP VPN Client	Opens the page for configuring the appliance as a PPTP VPN client. See “PPTP VPN Client” on page 349.
PPTP VPN Server	Opens the page for configuring the appliance as a PPTP VPN server. See “PPTP VPN Server” on page 352.
L2TP VPN Client	Opens the page for configuring the appliance as an L2TP VPN client. See “L2TP VPN Client” on page 373.
L2TP VPN Server	Opens the page for configuring the appliance as an L2TP VPN server. See “L2TP VPN Server” on page 363.
IPSec	Opens the pages for configuring IP Security (IPSec). See “IPSec example” on page 410.
Port Tunnels	Opens the pages for configuring HTTP and SSL client and server port tunnels. See “Port tunnels” on page 452. <i>Note: Not applicable to the SG300 model.</i>

Table 11: System menu

System menu options	Description
Date and Time	Opens the Date and Time Configuration page where you can set date, time, and locality. See “Date and Time menu” on page 462.
Backup/Restore	Opens the available options for Configuration Backup/Restore for Remote, Local, and Text. See “Backup/Restore menu” on page 469.
Users	Opens the Administrative users page where you can add or edit users and their permissions. See “Users menu” on page 476.
Management	Opens the CommandCenter Management page. See “Management menu” on page 486.
Diagnostics	Opens the Diagnostics page where you can view system information, system log information, perform networks tests, view USB devices (SG565 only), and capture network traffic. See “Diagnostics menu” on page 497.
Advanced	Opens the advanced features for Reboot / Configuration such as Reboot, Flash Upgrade, upload and edit Configuration Files, and direct edit of the Device Configuration. See “Advanced menu” on page 511.
Help and Support	Opens the Technical Support page, where you can find additional sources of information or report an issue if you have a support agreement. See “Help and Support menu option” on page 26.

Interface icons

The icons in the SnapGear Management Console (Web GUI) provide navigation to Online Help page icon help pages, backup and restore pages, and editing pages for features.

Online help icon

To access context-sensitive help for the page you are currently viewing, click the help icon. For more information about the Help and Support menu option, see “Help and Support menu option” on page 26.

Figure 10: Help icon



Backup and restore icon

The Backup and restore icon is available from every page within the SnapGear management console. Clicking the icon opens the Remote Configuration Backup/Restore page. For information on backup and restore, see “Remote Backup/Restore page” on page 470.

Figure 11: Backup/
Restore icon



Edit and delete icons

Many of the pages in the SnapGear management console have icons with which you can edit or delete its associated definition. You can click the edit icon associated with the item you want to edit.

Figure 12: Edit icon



You can click the delete icon associated with the item you want to delete.

Figure 13: Delete icon



Add above and below icons

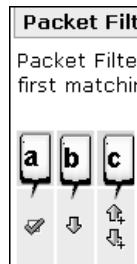
Certain pages within the Web console, such as for packet filtering and NAT rules, have icons you can use to add and manipulate the ordered list of objects within the pages. The add above or below icon has plus (+) signs next to the arrows, indicating you are adding an object. The arrow pointing upward adds the object above the current row selection; the arrow pointing downward adds the object below the current row.

Figure 14: Add above/
below icon



The controls you use to manipulate rules (and policy routes as well) are labelled in Figure 15:

Figure 15: Rule object
controls



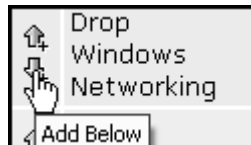
- a. Enable/disable check box
- b. Move rule up or down arrows
- c. Add rule above or below current rule location

Many of the pages in the console also have enable or disable check boxes as indicated in the above figure. The enable check box is the leftmost check box.

Tooltips

Hover your pointer over a control to view its tooltip.

Figure 16: Tooltip



Help and Support menu option

The Help and Support menu option opens the following pages:

- Online Help page
- Technical Support page
- Technical Support Report page

Online Help page

Use this page to access the help about the SnapGear online help page. From the **System** menu, click **Help and Support > Help** tab.

Figure 17: Online Help Search page

Technical Support page for additional resources.'" data-bbox="292 316 789 577"/>

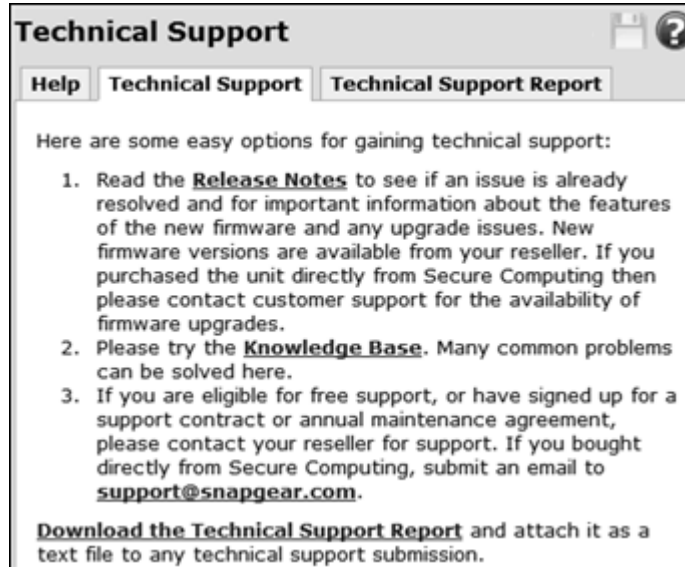
To access context-sensitive help for the page your are currently viewing, click the help icon. Help describes each field, along with acceptable input values where appropriate.

To search the entire contents of the help system, enter terms in the **Keywords** field and click **Search**. The search results are displayed in the page. Click a link to view its associated topic. The Search field is available on every help page.

Technical Support page

To access the technical support page, from the **System** menu, click **Help and Support > Technical Support** tab. The Technical Support page appears.

Figure 18: Technical Support page



This page provides links to the release notes, the knowledgebase, and the Technical Support Report to assist technical support staff with troubleshooting the configuration of your appliance. You can click the email link to technical support to launch an addressed email within your default mail program. Be sure to download and attach the technical support report. See "Technical Support Report page" on page 28.

Technical Support Report page

The Technical Support Report page is an invaluable resource for the technical support team to analyze problems with your SnapGear appliance. The information on this page gives the support team important information about any problems you may be experiencing with your appliance.

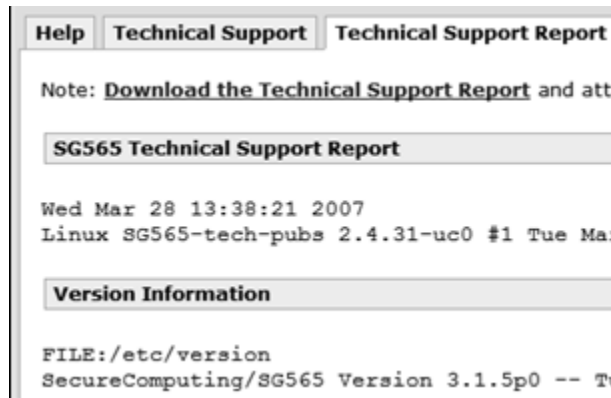
Note: To maintain your security and privacy, the technical support report removes any confidential information such as passwords and keys.

If you experience a fault with your appliance and have to contact the technical support team, ensure you include the Technical Support Report with your support request. The Technical Support Report should be generated when the issue is occurring on each of the appliances involved, and attached in plain text format. Otherwise, the Secure Computing technical support staff are unlikely to have enough information to assist you. When you submit a support request, be sure to attach the Technical Support Report.

To generate the technical support report:

- 1 From the **System** menu, click **Help and Support > Technical Support Report** tab. The Technical Support Report page appears.

Figure 19: Technical Support Report page



- 2 Click the [Download the Technical Support Report](#) link.
- 3 Save the report as a text file.

SnapGear Portal

You can access the SnapGear Portal using the following URL:

<http://sgkb.securecomputing.com>

No special account or log in is required to access the portal. The SnapGear Portal provides you with links to knowledgebase articles. You can search for articles, review articles, or request a new article. Free Web-based training is available. You can also log a support ticket in the Web ticketing interface.

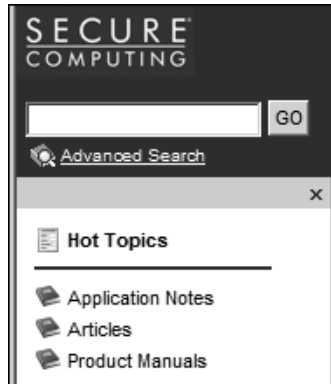
Figure 20: SnapGear Portal



The KB contains links to hot topics, latest articles, and has search capabilities. The **Hot Topics** pane contains the most frequently accessed articles. You can subscribe to an article by clicking the **Subscribe** link. Any updated articles to which you are subscribed are e-mailed to you.

You can also access product manuals, release notes, and application notes in the navigation area shown in Figure 21:

Figure 21: Portal navigation area

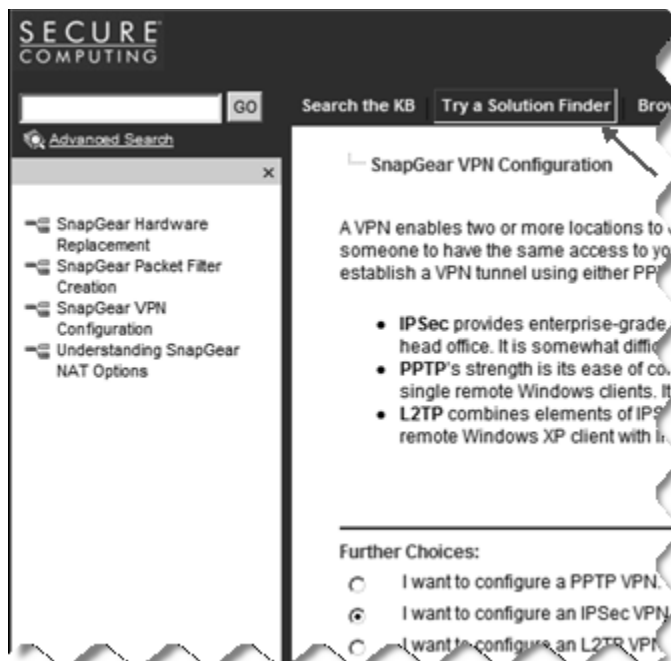


You can search by keyword, or if you know the article number as provided in certain topics within this guide, enter the article number and click **GO**.

Solution Finder

Click the **Try a Solution Finder** tab to step through guided configuration options for features such as NAT, packet filters, and VPN.

Figure 22: Solution Finder



CHAPTER 2

Network Setup Menu Features

Network setup overview	34
Connections	35
ADSL	46
Connecting with a cable modem	55
Configuring a dialout connection on the COM port	59
Setting up dial-in access	66
Failover, load balancing, and high availability	75
Internet connection failover	77
Load balancing	83
High Availability	86
DMZ network	94
Guest network	97
Wireless	99
Bridging	119
VLAN	127
GRE tunnels	136
Troubleshooting GRE tunnels	138
Routes	139
Example: OSPF	146
Example: BGP	149
System tab	151
DNS	153
DHCP Server	162
Web cache	176
QoS Traffic Shaping	190
SIP Proxy tab	198

Network setup overview

This chapter describes the Network Setup options of the SnapGear management console. Use the Network Setup options to configure each of your SnapGear appliance's Ethernet, wireless, and serial ports:

- An Ethernet network interface can be configured to connect to your LAN, DMZ, an untrusted LAN, or the Internet as a primary, backup, or load-balancing connection.
- A serial port can be configured to provide remote dial-in access, or connect to the Internet as a primary or back-up connection.
- A wireless interface can be configured to connect to your LAN, DMZ, or an untrusted LAN.

If you are using a SnapGear gateway or rack mount appliance, the appropriate quick installation guide gives instructions for configuring the PCs on your LAN to share the connection once your Internet connection has been established.

Multifunction vs. fixed-function ports

Some SnapGear appliances have network ports with labels corresponding to the port's function, such as LAN, DMZ, and Internet/WAN. These are said to be fixed-function ports.

Alternatively, some SnapGear appliances have network ports that are generically labeled; for example, port A, port B, port C. These are said to be multifunction ports. This reflects the ability of these ports to perform different functions; for example, port B is not limited to connecting to the Internet only, it can be configured as a LAN connection. Before configuring multifunction ports, determine which function you are assigning to each of the ports.

The SG560, SG565, and SG580 models have generically named Ethernet ports (ports A1, A2, A3, A4 and B). By default, switch A functions as a regular LAN switch, with network traffic passing freely between its ports. Typically, port B is used as your primary Internet connection. However, switch A's ports can be configured individually to perform separate functions. For example, port A2 can be configured to connect to a second LAN, port A3 can be configured as a DMZ port, and port A4 can be configured as a secondary Internet connection. These per-port configuration scenarios are accomplished using VLANs (Virtual Local Area Networks). For information about the advanced use of the VLAN capability of your SnapGear appliance, refer to "VLAN" on page 127 and "Port-Based VLANs" on page 129.

Connections

Under the Connections tab, each of your SnapGear appliance's network interfaces display alongside its physical Port name and the Current Details of its configuration.

Initially, all network interfaces are unconfigured, aside from a single LAN connection on the initial setup port (Switch **A** on SnapGear rack mount appliances SG560, SG565, and SG580; the **LAN** port on other models).

This page displays a list of the physical and virtual network interfaces of the SnapGear unit, as well as the network connections that have been configured for these interfaces.

Network interfaces can be physical interfaces such as Ethernet ports or serial ports. They can also be virtual interfaces such as bridges, GRE tunnels, or VLANs.

To configure a network connection, you need to specify the configuration details that will enable the network interface to be used for routing. The simplest network connections are static or dynamic IP addresses. More advanced network connections allow you to communicate with cable, ADSL, or serial modems that are connected to your SnapGear appliance.

Figure 23: Network Setup Connections page

	Name	Port	Current Details	Change Type	
<input checked="" type="checkbox"/>	Switch A	A	LAN, Static, 192.168.0.1	Direct Connection	
	Switch A VLAN 1234	A	VLAN 1234, Unconfigured	Unconfigured	
<input checked="" type="checkbox"/>	Port B	B	Internet, Static, 10.10.57.200	Direct Connection	
<input checked="" type="checkbox"/>	COM1	COM1	Internet	Dialout	
<input checked="" type="checkbox"/>	WIFI	Wireless	LAN, Static, 172.16.1.1	Direct Connection	

Retry unsuccessful connections **Retry**

Add Bridge

A network interface is configured or changed by selecting a connection type from the **Change Type** list.

Click **Retry** to immediately retry any connections that are currently down or have completely failed.

You can create new virtual network interfaces by selecting an option from the list and clicking **Add**.

Viewing or editing a connection

The current configuration for a connection can be viewed or edited by clicking its edit icon.

- 1 From the **Network Setup** menu, click **Network Setup**. The Network Setup Connections tab appears.
- 2 Select the edit icon for the connection your want to edit. The main configuration page appropriate for the connection appears.
- 3 Make your changes and click **Update**. You can also make changes in the additional tabs that appear for a connection, such as Aliases and IPv6. For more information, see “Aliases tab” on page 43 and “Enabling IPv6 for a connection” on page 44.

Disabling a connection

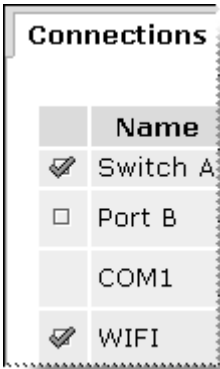
- 1 From the **Network Setup** menu, click **Network Setup**. The Network Setup Connections tab appears.
- 2 Select the enable check box for the connection. There should be a check mark present.
- 3 You are prompted to confirm disabling the connection. Click **OK**. The check mark no longer appears in the leftmost column.

Enabling a connection

Use this procedure to enable a disabled connection. A connection that can be re-enabled appears as an empty check box in the leftmost column.

- 1 From the **Network Setup** menu, click **Network Setup**. The Network Setup Connections tab appears.
- 2 Select the enable check box for the connection. The page refreshes and a check mark appears in the enable/disable column.

Figure 24: Enabled and disabled connections



Connections	
	Name
<input checked="" type="checkbox"/>	Switch A
<input type="checkbox"/>	Port B
	COM1
<input checked="" type="checkbox"/>	WIFI

Deleting a connection

Use this procedure to delete a connection configuration for a network interface.

Note: *You cannot delete the Direct Connection configuration for Switch A.*

If you delete a port-based VLAN, any ports assigned to that VLAN revert to the default VLAN of the switch. You can then reassign the port to a different VLAN using the VLAN Configuration tab of the VLAN. For further information, see “Editing a VLAN” on page 134.

- 1 From the **Network Setup** menu, click **Network Setup**. The Network Setup Connections tab appears.
- 2 Select the delete icon for the connection your want to delete. You are prompted to confirm the delete. Click **OK**.
- 3 If the connection was a virtual connection, the connection no longer appears in the Connections table. Otherwise, the **Change Type** column displays **Unconfigured** in its configuration list.

Direct connection overview

A direct connection is a direct IP connection to a network that does not require a modem to be established. This is typically a LAN, DMZ, or Guest connection, but it can also be an Internet connection. Network settings can be assigned statically, or dynamically by a DHCP server.

Direct connections can be added to a network bridge. For more information, see “Bridging” on page 119.

Direct Connection Settings page

Use this page to configure IP address settings for a direct connection.

- 1 From the **Network Setup** menu, click **Network Setup**. The Network Setup Connections tab appears.
- 2 Select the edit icon for the connection your want to edit. The main configuration page appropriate for the connection appears.
- 3 Click the **Direct Connection** tab. The Direct Connection Settings page appears.

Figure 25: Direct Connection page

The screenshot shows the 'Network Setup' window with the 'Direct Connection' tab selected. The 'Direct Connection Settings' section contains the following fields and options:

- Port:** A1, A2, A3, A4
- Current Details:** LAN, Static, 192.168.0.1
- Connection Name:** A text input field.
- DHCP assigned:** An unchecked checkbox.
- IP Address:** A text input field containing '192.168.0.1'.
- Subnet Mask:** A text input field containing '24'.
- Gateway:** A text input field.
- DNS Server(s):** A text input field.
- Firewall Class:** LAN
- Buttons:** 'Update' and 'Cancel' buttons at the bottom.

- 4 [Optional] Enter a descriptive name for the interface in the **Connection Name** field.
- 5 Perform one of the following options:
 - If you are using DHCP, select the **DHCP assigned** check box and skip to step 8. The appliance obtains its LAN network settings from an active DHCP server on your local network. Any values in the **IP Address**, **Subnet Mask**, and **Gateway** fields are ignored.

- If you are defining a static address, clear the check box and continue with the next step. You must define the IP address and Subnet Mask.
- 6** To assign network settings statically, enter an address in the **IP Address** field. If you are using the SnapGear appliance in its default network address translation mode, this is typically part of a private IP address range, such as *192.168.0.1 / 255.255.255.0*.
- 7** Enter the subnet mask you want to use for this port in the **Subnet Mask** field.
 - Range: 0-32; can also be in the form 255.255.255.0
- 8** If required, enter the IP address of the default **Gateway** out which to send outgoing traffic on this connection. If the default gateway is via the DMZ, define this setting. For LAN connections, a default gateway is not generally necessary.
- 9** [Conditional, if not using DHCP. Optional if using DHCP.] Enter one or more DNS servers the appliance uses for DNS resolution in the **DNS Servers** field. To enter multiple servers, separate each IP address with a comma. Any DNS server addresses allocated by the DHCP server take precedence over entries in this field.
- 10** Select a classification from the **Firewall Class** list. The Firewall class setting controls the basic allow/deny policy for this interface. Allowed network traffic is accepted, denied network traffic is dropped. Dropped means network traffic is denied silently; no response such as “connection refused” is sent back to the originator of the traffic.

The policy associated with each firewall class is detailed in Table 12. VPN and Dial-In connections are assigned a firewall class of LAN by default.

Table 12: Firewall class policy

Incoming Interface	Outgoing Interface	Action
LAN	Any	Accept
VPN	Any	Accept
Dial-in	Any	Accept
DMZ	Internet	Accept
DMZ	Any except Internet	Drop
Internet	Any	Drop
Guest	Any	Drop

For further discussion of DMZ and Guest networks, see “DMZ network” on page 94 and “Guest network” on page 97.

- 11** Click **Update**.

Ethernet Configuration tab

Use this procedure to modify the low-level Ethernet configuration settings of an Ethernet network port.

- 1 From the **Network Setup** menu, click **Network Setup**. The Network Setup Connections tab appears.
- 2 Select the edit icon for the connection your want to edit. The main configuration page appropriate for the connection appears.
- 3 Click the **Ethernet configuration** tab. The Configure Ethernet Port page appears.

Figure 26: Configure Ethernet Port

Network Setup

Connections

Failover & H/A

Routes

System

DNS

IPv6

Direct Connection

Ethernet Configuration

Aliases

IPv6

Configure Ethernet Port

Port

A1, A2, A3, A4

Name

Switch A

Current Details

LAN, Static, 192.168.0.1

MAC Address

00:D0:CF:04:F0:32

MTU

1500

Port

Ethernet Speed

A1

Default Auto Negotiation

A2

Default Auto Negotiation

A3

Default Auto Negotiation

A4

Default Auto Negotiation

Enable Port-based VLANs

☒

Default Port-based VLAN ID

2

Update

Cancel

- 4 On rare occasions, it may be necessary to change the Ethernet hardware or **MAC Address** of your SnapGear appliance. The MAC address is a globally unique address and is specific to a single SnapGear appliance. It is set by the manufacturer and should not normally be changed. However, you may need to change it if your ISP has configured your ADSL or cable modem to only communicate with a device with a known MAC address.

Enter a MAC address in the **MAC** field. The address can be an Ethernet MAC address of the form AA:BB:CC:DD:EE:FF, where each of the components is a hexadecimal digit.

Note: This setting cannot be changed for the LAN port or Port A.

Figure 27: Configure Ethernet Port-MAC address

The screenshot shows the 'Network Setup' window with the 'Ethernet Configuration' tab selected. The 'Configure Ethernet Port' section is active, displaying the following settings: Port B, Name Port B, Current Details Internet, Static, 10.10.57.200, MAC Address 00:D0:CF:04:F0:33, MTU 1500, and Ethernet Speed set to Default Auto Negotiation. There are 'Update' and 'Cancel' buttons at the bottom.

- 5 [Optional] If an Ethernet port is experiencing difficulties auto-negotiating with another device, you can manually set Ethernet speed and duplex from the **Ethernet Speed** list. Available options are:
- **Default Auto Negotiation**
 - **100 Base Tx - Auto Duplex**
 - **100 Base Tx - Full Duplex**
 - **100 Base Tx - Half Duplex**
 - **10 BaseT - Auto Duplex**
 - **10 BaseT - Full Duplex**
 - **10 BaseT - Half Duplex**
 - **100 Base T4**
- 6 Specify the MTU (Maximum Transfer Unit) for the interface in the **MTU** field. This setting should normally be left at 1500.

Note: This setting only effects the Ethernet interface, and does not change the MTU for ADSL PPPoE interfaces.

- Can be an integer equal to or greater than 1

- 7 [Optional] To enable the VLANs of the switch, select the **Enable Port-based VLANs** check box. When enabled, each port in the switch can be assigned to different VLANs. The primary reason for using port-based VLANs is to isolate each port in the switch. This allows you to connect different networks to each port, and to enforce firewall policies between ports. After enabling port-based VLANs, you need to create VLANs on the Connections page, modify the VLANs, and assign ports to each VLAN on the VLAN Configuration tab. Any ports that are left unassigned will use the default VLAN as described below. Port 1 will always use the default VLAN. You can also use the Quick Setup Wizard to automatically create separate VLANs for each port. After disabling port-based VLANs, any VLANs you have created will remain as tagged VLANs. You should delete them if they are unneeded.
- 8 Specify the default VLAN ID for this switch in the **Default Port-based VLAN ID** field. This field is only required when port-based VLANs are enabled, and must be unique amongst the VLANs on this switch. If a port is disabled for all VLANs, then the port will be set to untagged mode for the default VLAN. The untagged mode means the VLAN ID will only be used while routing packets within this appliance. Devices connected to ports on the default VLAN will not see the VLAN ID on the packet, and do not need to support VLANs. Therefore the actual value is irrelevant, as long as it is unique.
 - Range: 1-4094
 - Can be blank
 - Must be unique
- 9 Click **Update**.

Aliases tab

Alias addresses are typically assigned to an Internet network connection. Alias addresses enable you to use the same TCP or UDP port for multiple servers. Interface aliases allow the SnapGear appliance to respond to multiple IP addresses on a single network interface. This is useful for when your ISP has assigned you a range of IP addresses to use with your Internet connection, or when you have more than one subnet connected to a single network interface.

Figure 28: Aliases tab

The screenshot shows the 'Network Setup' window with the 'Aliases' tab selected. The 'Interface Aliases' section displays the following details:

Alias IP Address	Alias Subnet Mask	Delete
1.1.1.1	24	

Below the table, there are input fields for 'Alias IP Address' and 'Alias Subnet Mask', both currently showing '24'. At the bottom are 'Add' and 'Cancel' buttons.

For aliases on interfaces that have the DMZ or Internet firewall class, you must also setup appropriate packet filtering or port forwarding rules to allow traffic on these ports to be passed from the alias address to servers on the local network. For details, see “Packet Filter Rules page” on page 232 and “About port forwarding” on page 245.

Adding an alias IP address for an interface

- 1 From the **Network Setup** menu, click **Network Setup**. The Network Setup Connections tab appears.
- 2 Select the edit icon for the connection you want to edit. The main configuration page appropriate for the connection appears.
- 3 Click the **Aliases** tab.
- 4 Enter the alias address in the **Alias IP Address** field.
- 5 Enter the alias subnet mask in the **Alias Subnet Mask** field.
 - Range: 0-32; can also be in the form 255.255.255.0

- 6 Click **Add**. The alias is added to the list of for the interface.

Deleting an alias IP address for an interface

- 1 From the **Network Setup** menu, click **Network Setup**. The Network Setup Connections tab appears.
- 2 Select the edit icon for the connection your want to edit. The main configuration page appropriate for the connection appears.
- 3 Click the **Aliases** tab.
- 4 Click the delete icon for the alias IP address you want to delete. The alias is deleted from the list.

Enabling IPv6 for a connection

Use this procedure to enable IPv6 for a connection. In particular, enable IPv6 for the LAN connections on which you want to advertise routes, and on the Internet connections on which you want to create 6to4 tunnels.

To route and filter IPv6 traffic, you must also enable IPv6 at the appliance level. For details, refer to “IPv6 tab” on page 196 and “Enabling IPv6 at the appliance level” on page 196.

- 1 From the **Network Setup** menu, click **Network Setup**. The Network Setup Connections tab appears.
- 2 Select the edit icon for the connection your want to edit. The main configuration page appropriate for the connection appears.
- 3 Click the **IPv6** tab.

Figure 29: IPv6 connection level

The screenshot shows the 'Network Setup' window with the 'IPv6' tab selected. The 'Ethernet Configuration' sub-tab is active. The configuration details for 'Switch A' are shown, including 'Current Details' as 'LAN, Static, 192.168.0.1'. The 'Enable IPv6' checkbox is checked, and the 'Site Level Aggregation' is set to 0. 'Update' and 'Cancel' buttons are at the bottom.

Network Setup	
Connections Failover & H/A Routes System DNS IPv6	
Direct Connection Ethernet Configuration Aliases IPv6	
Name	Switch A
Current Details	LAN, Static, 192.168.0.1
Enable IPv6	<input checked="" type="checkbox"/>
Site Level Aggregation	0
Update Cancel	

- 4 Select the **Enable IPv6** check box.

- 5 [LAN connections only] You can enter a site level aggregation value for this connection in the **Site Level Aggregation** field. This field is used to create a site-local address for this connection, and is also used for creating routes for any 6to4 tunnels. This setting should be unique.
 - Can be from 1 to 4 hexadecimal characters (0-9, a-b, A-B)
 - Default: 0
- 6 Click **Update**.

Disabling IPv6 for a connection

Use this procedure to disable IPv6 for a connection. If you want to disable IPv6 for all connections, disable IPv6 at the appliance level. For more information, see “Disabling IPv6” on page 197.

- 1 From the **Network Setup** menu, click **Network Setup**. The Network Setup Connections tab appears.
- 2 Select the edit icon for the connection your want to edit. The main configuration page appropriate for the connection appears.
- 3 Click the **IPv6** tab.
- 4 Clear the **Enable IPv6** check box.
- 5 Click **Update**.

ADSL

This topic contains procedures for configuring your DSL connection, also referred to as ADSL (Asymmetric Digital Subscriber Line). ADSL connections have the interface firewall class of *Internet*.

Routed versus bridged DSL modems

Before you configure ADSL, check whether your DSL modem is in a routed or bridged mode. Many ISPs preconfigure this for your convenience. Often you can change the mode to suit your needs. Check with your ISP to determine if they can accommodate changing between bridged and routed mode or vice versa on the modem they supplied.

If your DSL modem is in routed mode, then all PPTP/PPPoE and similar login and connection considerations are addressed from inside the modem. You should then connect your SnapGear appliance in Direct or DHCP mode to your DSL modem, and will not be required to enter any additional ADSL information on the SnapGear management console.



Important: Do not use ADSL configuration on the SnapGear management console if your modem is in routed mode.

There are some advantages to the bridged mode:

- Your SnapGear appliance becomes the portal to the Internet
- You do not have to port-forward service in two places (on the DSL modem and on the SnapGear appliance).

The ADSL configurations listed here generally work best when your DSL modem is in bridged mode.

Note: PPPoA is not supported. If your ISP only supports PPPoA, the DSL modem must be configured in routed mode. For further information, see article #2708 in the SnapGear KB <http://sgkb.securecomputing.com>.

If your ISP only support PPPoA, the SnapGear appliance needs to be configured with either DHCP or a static address so it can communicate with the upstream router, which is your DSL modem.

ADSL configuration methods

You can configure DSL to establish a connection to your ISP using the following methods:

- **Auto detect:** If you are unsure of your ADSL connection type, the SnapGear appliance can attempt to Auto detect ADSL connection type. The appliance is unable to detect the PPTP connection type. Refer to the procedure “Autodetecting your ADSL connection” on page 49.
- **PPPoE:** Select this method if your ISP uses user name and password authentication to access the Internet. Refer to the procedure “Connecting ADSL via PPPoE” on page 50.
- **PPTP:** Select this method if you have a dial-up VPN connection to the Internet provided by your ISP. Refer to the procedure “Connecting ADSL via PPPT” on page 51.
- **DHCP:** Select this method if your ISP does not require a user name and password, or your ISP provides a dynamic IP address. Refer to the procedure “Connecting ADSL via DHCP” on page 52.
- **Manually Assign Settings:** Select this method if your ISP has given you a static IP address or address range. Refer to the procedure “Manually assigning your ASDL settings” on page 53.

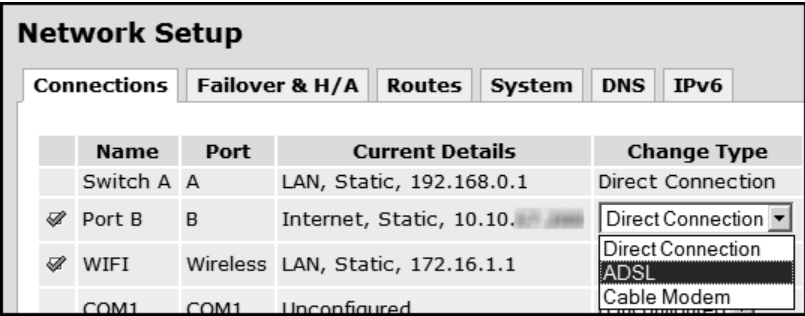
Prerequisites:

- 1 If you have not already done so, connect the appropriate network port of your SnapGear appliance to your DSL modem.
- 2 Power on the DSL modem and give it some time to initialize. Ensure the Ethernet link LEDs are illuminated on both the SnapGear appliance (if applicable to the model) and DSL modem. Do not continue until it has reached the line sync state and is ready to connect. Most modems have a sync/line sync LED that indicates whether or not the modem is talking to the DSLAM (Digital Subscriber Line Access Multiplexer) of the telephone exchange. For more information on LEDs, refer to the appropriate LED topic for your SnapGear model in Chapter 1, Introduction.
- 3 Access the ADSL connections page so that you can configure your DSL connection. See “Accessing the ADSL connection methods page” on page 48.

Accessing the ADSL connection methods page

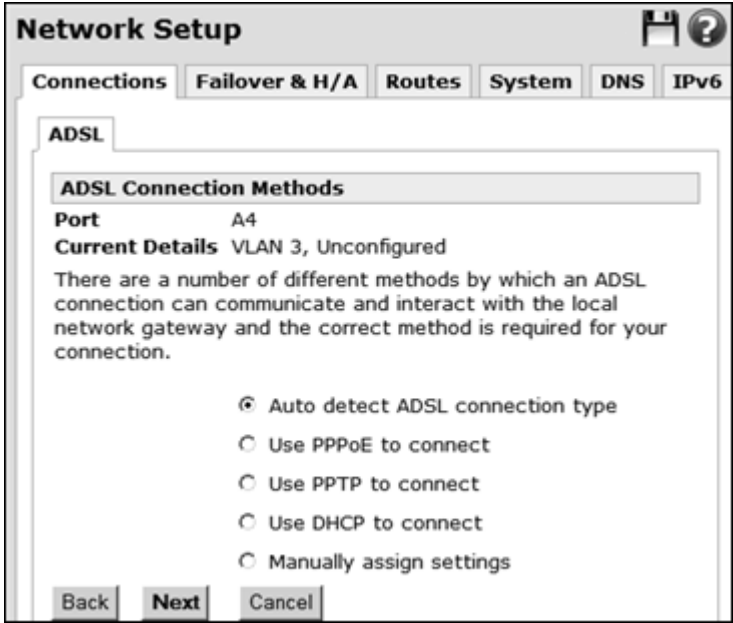
- 1 From the **Network Setup** menu, click **Network Setup**. The **Connections** page appears.

Figure 30: ADSL Connection Details



- 2 For the connection you want to configure ADSL on, select **ADSL** from the **Change Type** list. Not all connections have this option available, such as the COM serial port. The ADSL tab opens and displays the ADSL Connection Methods page.

Figure 31: ADSL Connection Methods



- 3 Select the connection method you need to use and click **Next**.

- 4 Continue with the procedure you need to use to connect:
 - “Autodetecting your ADSL connection” on page 49
 - “Connecting ADSL via PPPoE” on page 50
 - “Connecting ADSL via PPPT” on page 51
 - “Connecting ADSL via DHCP” on page 52
 - “Manually assigning your ASDL settings” on page 53

Autodetecting your ADSL connection

Use this procedure to autodetect settings for your ADSL. Autodetect does not work for PPPT connections.

- 1 Click **Network Setup > Network Setup**. On the **Connections** page, select **ADSL** from the **Change Type** list. The ADSL Connection Methods page appears.
- 2 Select the **Auto detect ADSL connection type** option and click **Next**.
- 3 A message reminds you to hook up your equipment. Click **Next**.
- 4 Depending on what the appliance detects, either the ADSL DHCP Configuration page appears (see Figure 34 on page 53), or the PPPoE page appears (Figure 32 on page 50).
- 5 Complete the fields and click **Finish**.

If autodetect succeeds, additional configuration tabs appear, such as the VLAN configuration or Ethernet configuration tab (depending on your connection type), Aliases, and IPv6. See “Ethernet Configuration tab” on page 40, “VLAN” on page 127, “Aliases tab” on page 43, and “Enabling IPv6 for a connection” on page 44.

If autodetection fails, your DSL modem might not be configured correctly for your connection type, or your DSL service has not yet been provisioned by your telecommunications company. Try the manual settings procedure as well.

Connecting ADSL via PPPoE

Figure 32: ADSL PPPoE
Configuration

Use this procedure to configure your ADSL for a PPPoE connection.

- 1 Click **Network Setup > Network Setup**. On the **Connections** page, select **ADSL** from the **Change Type** list. The ADSL Connection Methods page appears.
- 2 Select the **Use PPPoE to connect** option and click **Next**. The ADSL PPPoE Configuration page appears.

The screenshot shows the 'Network Setup' window with the 'Connections' tab selected. Under the 'ADSL' section, the 'ADSL PPPoE Configuration' sub-tab is active. The 'Port' is set to 'B'. The 'Current Details' are 'Internet, Static,'. A text block instructs the user to configure their PPPoE ADSL Internet connection and mentions that service providers usually supply a username and password. Below this, there are four input fields: 'Connection Name', 'Username', 'Password', and 'Confirm Password'. At the bottom of the configuration area are three buttons: 'Back', 'Finish', and 'Cancel'.

- 3 [Optional] Enter a descriptive name in the **Connection Name** field.
- 4 Enter the username from your ISP in the **Username** field.
- 5 Enter the password from your ISP in the **Password** field.
- 6 Enter the password again in the **Confirm Password** field.
- 7 Click **Finish**.

By default, PPPoE connections are treated as always on and are kept up continuously. Alternatively, you can choose to only bring the connection up when PCs on the LAN, DMZ, or Guest network (via a VPN tunnel) are trying to reach the Internet. For instructions, refer to “Enabling dial on demand for a connection” on page 63. Since DSL connections are not generally metered by time, this is rarely a desirable configuration due to the delays when initiating the on-demand connection.

After you click Finish, additional configuration tabs appear, such as the VLAN configuration or Ethernet configuration tab (depending on your connection type), Aliases, and IPv6. See “Ethernet Configuration tab” on page 40, “VLAN” on page 127, “Aliases tab” on page 43, and “Enabling IPv6 for a connection” on page 44.

Connecting ADSL via PPPT

Use this procedure to configure a PPTP DSL connection to your ISP.

- 1 Click **Network Setup > Network Setup**. On the **Connections** page, select **ADSL** from the **Change Type** list. The ADSL Connection Methods page appears.
- 2 Select the **Use PPPT to connect** option and click **Next**. The ADSL PPTPoE Configuration page appears.

Figure 33: ADSL PPTPoE Configuration

The screenshot shows the 'Network Setup' window with the 'Connections' tab selected. Under the 'ADSL' sub-tab, the 'ADSL PPTPoE Configuration' section is active. It displays the following fields and options:

- Port:** B
- Current Details:** Internet, Static,
- Instructions:** Configure your PPTP ADSL Internet connection. Your service provider should have supplied you with a username, password and PPTP server IP address to use to connect to the Internet. Also provide a local IP address and netmask that will be used to connect to the PPTP server.
- Connection Name:** [Empty text box]
- Username:** [Empty text box]
- Password:** [Empty text box]
- Confirm Password:** [Empty text box]
- PPTP Server IP Address:** [Empty text box]
- Local IP Address:** [Empty text box]
- Subnet Mask:** 24 [Empty text box]
- Buttons:** Back, Finish, Cancel

- 3 [Optional] Enter a descriptive name in the **Connection Name** field.
- 4 Enter the username from your ISP in the **Username** field.
- 5 Enter the password from your ISP in the **Password** field.
- 6 Enter the password again in the **Confirm Password** field.
- 7 Enter the enter the PPTP server address provided by your ISP in the **PPTP Server IP Address** field.

- 8 Enter a local IP address in the **Local IP Address** field. The local IP address is used on the SnapGear appliance's network port through which you connect to the Internet.

Note: *In general, this is not your actual Internet IP address, but is the IP address the PPTP client uses as its source address. Once the PPTP client has established a connection with the ISP's PPTP server, the ISP allocates an address that is used as the actual Internet interface on the SnapGear appliance. Usually the address supplied by the ISP is different from the local IP address entered here. Even if the DSL modem is in bridged mode, it typically has allocated an administrative IP address, such as 192.168.1.1 or similar, so the DSL modem can be administered. It is recommended to set the local address to an IP on that same subnet, such as 192.168.1.2.*

- 9 Enter the netmask for the SnapGear network port through which you are connecting to the Internet in the **Subnet Mask** field. The netmask and the local address should be compatible with the LAN port settings on the DSL modem.

- 10 Click **Finish**.

Additional configuration tabs appear, such as the VLAN configuration or Ethernet configuration tab (depending on your connection type), Aliases, and IPv6. See "Ethernet Configuration tab" on page 40, "VLAN" on page 127, "Aliases tab" on page 43, and "Enabling IPv6 for a connection" on page 44.

Connecting ADSL via DHCP

Use this procedure to connect your ADSL via a DHCP configuration. Your ISP might require a Hostname; otherwise all other settings are assigned automatically by your ISP.

- 1 Click **Network Setup > Network Setup**. On the **Connections** page, select **ADSL** from the **Change Type** list for the interface you want to configure. The ADSL Connection Methods page appears.
- 2 Select the **Use DHCP to connect** option and click **Next**. The ADSL DHCP Configuration page appears.

Figure 34: ADSL DHCP Configuration page

The screenshot shows a web-based configuration interface titled "Network Setup". At the top, there are several tabs: "Connections", "Failover & H/A", "Routes", "System", "DNS", and "IPv6". The "Connections" tab is selected. Below the tabs, there is a sub-tab labeled "ADSL". Under the "ADSL" sub-tab, there is a section titled "ADSL DHCP Configuration". This section contains the following information:

- Port:** B
- Current Details:** Internet, Static,

Configure your DHCP ADSL Internet connection.

Some ADSL modems require that the connecting machine sends its hostname as part of the DHCP request. Leaving this field blank will send no hostname.

Below this text are two input fields:

- Connection Name:** An empty text box.
- Hostname:** An empty text box.

At the bottom of the configuration section are three buttons: "Back", "Finish", and "Cancel".

3 [Optional] Enter a descriptive name in the **Connection Name** field.

4 Enter the host name in the **Hostname** field.

5 Click **Finish**.

Additional configuration tabs appear, such as the VLAN configuration or Ethernet configuration tab (depending on your connection type), Aliases, and IPv6. See "Ethernet Configuration tab" on page 40, "VLAN" on page 127, "Aliases tab" on page 43, and "Enabling IPv6 for a connection" on page 44.

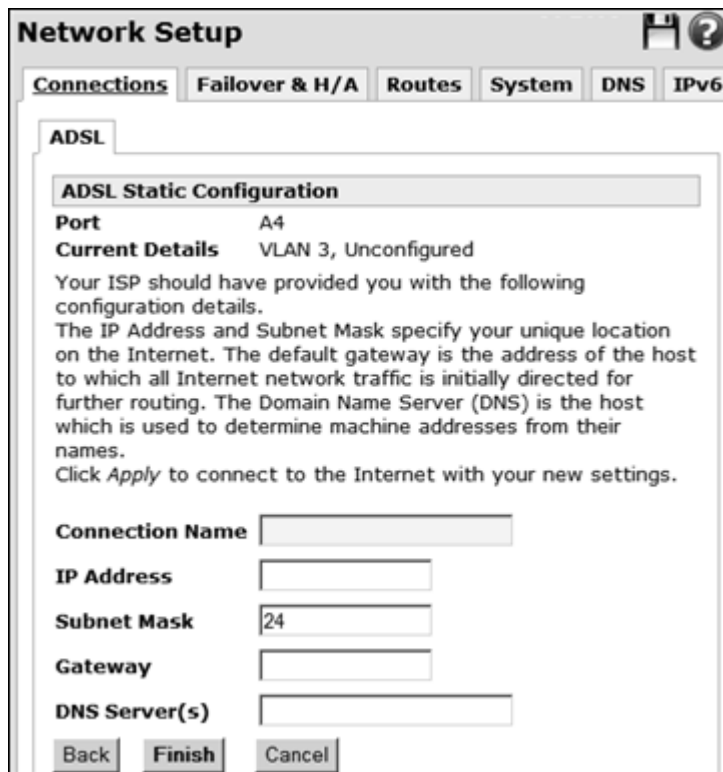
Manually assigning your ASDL settings

Use this procedure to manually configure your ADSL connection.

1 Click **Network Setup > Network Setup**. On the **Connections** page, select **ADSL** from the **Change Type** list. The ADSL Connection Methods page appears.

2 Select the **Manually assign settings** option and click **Next**. The ADSL Static Configuration page appears.

Figure 35: ADSL Static Configuration



The screenshot shows a web-based configuration interface titled "Network Setup". At the top, there are tabs for "Connections", "Failover & H/A", "Routes", "System", "DNS", and "IPv6". The "Connections" tab is selected, and within it, the "ADSL" sub-tab is active. The main content area is titled "ADSL Static Configuration". It displays the following information: "Port" is set to "A4", and "Current Details" are "VLAN 3, Unconfigured". A paragraph of text explains that the user's ISP should provide configuration details, including IP Address, Subnet Mask, Gateway, and DNS Server(s). Below this text, there are input fields for "Connection Name", "IP Address", "Subnet Mask" (with "24" entered), "Gateway", and "DNS Server(s)". At the bottom of the form are three buttons: "Back", "Finish", and "Cancel".

- 3 [Optional] Enter a descriptive name in the **Connection Name** field.
- 4 Enter the IP address provided by your ISP in the **IP Address** field.
- 5 Enter the IP address of the gateway provided by your ISP in the **Subnet mask** field.
- 6 Enter the IP address of the gateway provided by your ISP in the **Gateway** field.
- 7 Enter the **DNS Address** provided by your ISP in the **DNS Server** (or Servers) field. Separate multiple DNS addresses with commas.

- 8 Click **Finish**. Additional configuration tabs appear, such as the VLAN configuration or Ethernet configuration tab (depending on your connection type), Aliases, and IPv6. See “Ethernet Configuration tab” on page 40, “VLAN” on page 127, “Aliases tab” on page 43, and “Enabling IPv6 for a connection” on page 44.

Connecting with a cable modem

Use this procedure to connect to the Internet using a cable Internet service. Cable Modem connections have the interface firewall class of *Internet*.

Prerequisites: If you have not already done so, connect the appropriate network port of your SnapGear appliance to your cable modem. Power on the cable modem and give it some time to initialize. Ensure the Ethernet link LEDs are illuminated on both the SnapGear appliance (if applicable) and cable modem.

- 1 From the **Network Setup** menu, click **Network Setup**. The **Connections** tab opens.

Figure 36: Cable Modem Connection Details

Network Setup				
Connections				
Failover & H/A				
Routes				
System				
DNS				
IPv6				
	Name	Port	Current Details	Change Type
	Switch A	A	LAN, Static, 192.168.0.1	Direct Connection
<input checked="" type="checkbox"/>	Port B	B	Internet, Static, 10.10.57.200	Direct Connection
<input checked="" type="checkbox"/>	WIFI	Wireless	LAN, Static, 172.16.1.1	Direct Connection
	COM1	COM1	Unconfigured	ADSL
				Cable Modem

- 2 For the interface that you want to connect to your cable modem, select **Cable Modem** from the **Change Type** list.

- 3 The Cable Model Connection Details page appears. Select your cable ISP. If it is not **BigPond** or **@Home**, select the **Generic Cable Modem Provider** option.

Figure 37: Cable Modem Connection Details

The screenshot shows a web-based configuration interface titled "Network Setup". At the top, there are several tabs: "Connections", "Failover & H/A", "Routes", "System", "DNS", and "IPv6". The "Connections" tab is selected. Below the tabs, there is a sub-tab labeled "Cable Modem". The main content area is titled "Cable Modem Connection Details". It shows the "Port" as "A" and "Current Details" as "VLAN 1234, Unconfigured". A paragraph of text explains that most cable modems act as a simple DHCP server and that some require additional login authentication. It advises selecting the "Generic Cable Modem Provider" if the user's provider is not listed. A note mentions that the SnapGear unit will fail to acquire an IP address if the cable modem connection fails. Below this, there is a prompt to "Select your cable modem service provider" followed by three radio button options: "Generic Cable Modem Provider" (which is selected), "BigPond Advance (Australia)", and "@Home". At the bottom of the form are three buttons: "Back", "Next", and "Cancel".

- 4 Click **Next**.

The page that appears depends on your provider choice:

- If you chose **Generic Provider** as shown in Figure 38, enter a name for the connection in the **Connection Name** field [optional] and click **Finish**.

Figure 38: Generic Cable Modem Provider

The screenshot shows the 'Network Setup' window with the 'Connections' tab selected. Under the 'Cable Modem' section, 'Generic Cable Modem Provider' is chosen. The 'Port' is set to 'A' and 'Current Details' are 'VLAN 1234, Unconfigured'. A text block provides instructions: 'The SnapGear unit is ready to connect to your cable modem provider. Ensure that the cable modem Ethernet cable is inserted into the Internet interface at the back of the unit. Click the *Finish* button below when ready. If the connection is not established within several minutes, and you have checked it has been configured and physically connected correctly, unplug the cable modem's power cable for 5 - 30 minutes, reapply power, then reboot the SnapGear unit.' Below this is a 'Connection Name' text field and 'Back', 'Finish', and 'Cancel' buttons.

- If you chose **BigPond Advance** as shown in Figure 39, enter a **Connection Name** [optional], **Username**, and **Password**, and click **Finish**.

Figure 39: BigPond Advance Cable Modem Provider

The screenshot shows the 'Network Setup' window with the 'Connections' tab selected. Under the 'Cable Modem' section, 'BigPond Advance (Australia)' is chosen. The 'Port' is set to 'A' and 'Current Details' are 'VLAN 1234, Unconfigured'. A text block states: 'You now need to enter your BigPond Advance username and password'. Below this are four text fields: 'Connection Name', 'Username', 'Password', and 'Confirm Password'. At the bottom are 'Back', 'Finish', and 'Cancel' buttons.

- If you chose **@Home** as shown in Figure 40, enter a **Connection Name** [optional], **Hostname**, and click **Finish**.

Figure 40: @Home Cable Modem Provider

The screenshot shows a 'Network Setup' window with a tabbed interface. The 'Connections' tab is active, and within it, the 'Cable Modem' sub-tab is selected. A dropdown menu shows '@Home' as the selected provider. Below this, the 'Port' is set to 'A' and 'Current Details' show 'VLAN 1234, Unconfigured'. A text instruction states: 'You now need to enter your @Home host name (denoted DN on the yellow sheet provided with your @Home installation kit)'. There are two input fields: 'Connection Name' and 'Hostname'. At the bottom are three buttons: 'Back', 'Finish', and 'Cancel'.

Network Setup

Connections | Failover & H/A | Routes | System | DNS | IPv6

Cable Modem

@Home

Port: A

Current Details: VLAN 1234, Unconfigured

You now need to enter your @Home host name (denoted DN on the yellow sheet provided with your @Home installation kit)

Connection Name:

Hostname:

Back | **Finish** | Cancel

Configuring a dialout connection on the COM port



Use this procedure to configure a dialout Internet connection on the COM (serial) port of the SnapGear appliance. You can connect to the Internet using a regular dialup or ISDN service. Dialout and ISDN connections have the interface firewall class of *Internet*.

Caution: *Do not plug an ISDN connection directly into your SnapGear appliance. You must first connect a terminal adaptor.*

To connect to an ISDN line, the SnapGear appliance requires an intermediate device called a Terminal Adapter (TA). A TA connects to your ISDN line and has a serial port that connects to your SnapGear appliance.

Most ISDN TAs work with the SnapGear appliance; however, you might need to modify some files to use an appropriate initialization string to send to the modem. For more information on supported ISDN TAs and those that require additional manual configuration, consult article **#2742** in the SnapGear KB:

<http://sgkb.securecomputing.com>

By default, Dialout/ISDN connections are treated as always on and are kept up continuously. Alternatively, you can choose to only bring the connection up when PCs on the LAN, DMZ, or Guest network (via a VPN tunnel) are trying to reach the Internet. For instructions, refer to “Enabling dial on demand for a connection” on page 63.

Note: *Concurrent Dialin and Dialout configurations are not supported at this time.*

- 1 From the **Network Setup** menu, click **Network Setup**. The **Connections** page appears.
- 2 Select **Dialout** from the **Change Type** list for the COM1 interface that connects to your dialup modem or ISDN TA. The Dialout Account Details page appears.

Figure 41: Dialout-
Account Details

The screenshot shows a 'Network Setup' window with a 'Dialout' tab selected. Under the 'Account Details' section, there is a text box for 'Connection Name' and several other fields: 'Phone Number(s) to Dial', 'DNS Server(s)', 'Domain', 'Username', 'Password', and 'Confirm Password'. The 'Port' is set to 'COM1' and 'Current Details' are 'Unconfigured'. There are 'Finish' and 'Cancel' buttons at the bottom.

Field	Value
Port	COM1
Current Details	Unconfigured
Connection Name	
Phone Number(s) to Dial	
DNS Server(s)	
Domain	
Username	
Password	
Confirm Password	

- 3 [Optional] Enter a descriptive name, such as the name of your ISP, in the **Connection Name** field.
- 4 Enter the phone number in the **Phone Number(s) to Dial** field.

If your ISP has provided multiple phone numbers, you can enter them separated with commas. Use a backslash (\) to send a comma (pause) to your modem. For example, if you need to dial 0 to get an outside line from behind a PABX, and your ISP's number is 1234567, the Phone Number entry would be: 0\, \, \, 1234567. Other accepted characters include:

 - double-quotes (")
 - pound sign (#)
 - star sign (*)
- 5 [Optional] Enter the DNS server address provided by your ISP in the **DNS Server(s)** field. Separate multiple address with commas. Any DNS addresses automatically handed out by your ISP take precedence over addresses specified in this field.
- 6 [Optional] If the remote network has a Windows domain server, you might need to specify it to authenticate. Enter the domain in the **Domain** field.
- 7 Enter the username allocated by the ISP provider in the **Username** field.
- 8 [Optional] Enter the password provided by your ISP in the **Password** field.

Enter the password again in the **Confirm Password** field.

9 Click Finish.

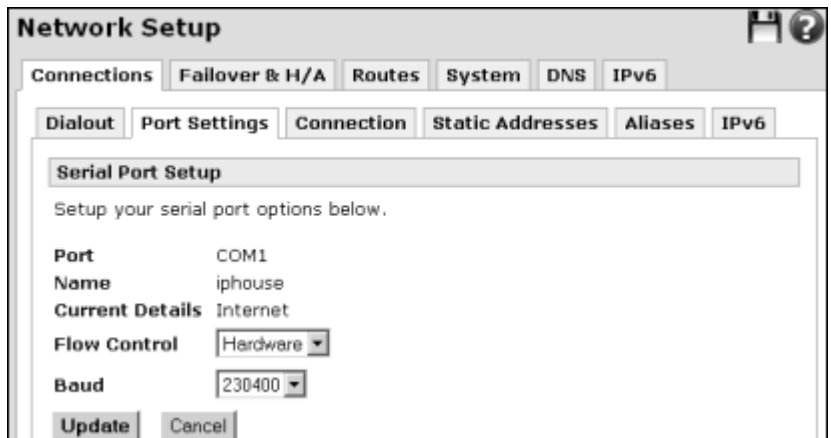
If necessary, you can continue to configure additional settings by clicking the **Port Settings**, **Connection**, **Static Addresses**, **Aliases**, and **IPv6** tabs for the serial port connection. See “Configuring dialout port settings” on page 61, “Enabling dial on demand for a connection” on page 63, “Configuring static IP addresses for a connection” on page 64, “Aliases tab” on page 43, and “Enabling IPv6 for a connection” on page 44.

Configuring dialout port settings

Use this procedure to configure dialout port settings. You can set the serial port Baud rate and Flow Control, but this is not usually necessary.

- 1 From the **Network Setup** menu, click **Network Setup**. The **Connections** tab opens. Click the edit icon for the Dialout connection.
- 2 Click the **Port Settings** tab. The Serial Port Setup page appears.

Figure 42: Port Settings-Serial Port Setup



The screenshot shows the 'Network Setup' window with the 'Connections' tab selected. Within this tab, the 'Port Settings' sub-tab is active. The 'Serial Port Setup' section contains the following fields: 'Port' set to 'COM1', 'Name' set to 'iphouse', 'Current Details' set to 'Internet', 'Flow Control' set to 'Hardware' (via a dropdown menu), and 'Baud' set to '230400' (via a dropdown menu). At the bottom of the form are 'Update' and 'Cancel' buttons.

- 3 Select the type of flow control to perform from the **Flow Control** list. Available options are:
 - **Hardware** — [Default. Most typical]. Requires the RTS/CTS (Request To Send/Clear To Send) pins on the serial interface to be appropriately connected to the other device.
 - **Software**

- 4 Select the baud rate of the serial interface from the **Baud Rate** list.
Available baud rates are:
 - **9600**
 - **19200**
 - **38400**
 - **57600**
 - **115200**
 - **230400**

Note: *This setting must match the baud rate of the device connected to the serial interface.*

- 5 Click **Finish**.

If necessary, you can continue to configure additional settings by clicking the **Connection**, **Static Addresses**, **Aliases**, and **IPv6** tabs for the serial port connection. See “Enabling dial on demand for a connection” on page 63, “Configuring static IP addresses for a connection” on page 64, “Aliases tab” on page 43, and “Enabling IPv6 for a connection” on page 44.

Enabling dial on demand for a connection

You can choose to bring up a PPPoE/PPPoA DSL, dialout, or ISDN connection only when PCs on the LAN, DMZ, or Guest network (via a VPN tunnel) are trying to reach the Internet and disconnect again when the connection has been idle for a specified period. This is known as *dial on demand*, and is particularly useful when your connection is metered by time.

Figure 43: Connection tab
— Dialout Connection
Settings Dial on demand

The screenshot shows the 'Network Setup' window with the 'Connections' tab selected. Within this tab, the 'Connection' sub-tab is active for a 'Dialout' connection. The 'Dialout Connection Settings' section includes the following fields and values:

Setting	Value
Port	COM1
Current Details	Internet
Dial on Demand	<input checked="" type="checkbox"/>
Idle Time (minutes)	15
Max Connection Attempts	4
Time between redials (seconds)	60
Debug Logging	<input type="checkbox"/>

At the bottom of the settings section are 'Update' and 'Cancel' buttons.

- 1 Click **Network Setup > Network Setup**. On the **Connections** page, click the **Edit** icon, then the **Connection** tab for the connection for which you want to enable dial on demand.
- 2 [Optional] To enable dial on demand, select the **Dial on Demand** check box.
- 3 In the **Idle Time** field, enter the number of minutes the appliance waits after the connection becomes idle before disconnecting.
 - Default: 15
 - Can be a value of zero or greater
- 4 In the **Max Connection Attempts** field, specify the number of times the appliance should attempt to make the connection.
 - Default: 4
 - Can be a value of zero or greater
- 5 In the **Time between redials (seconds)** field, enter the time to wait between connection attempts.
 - Default: 60
 - Can be a value of zero or greater

Disabling dial on demand for a connection

- 6 [Optional] To enable logging for debugging, select the **Debug Logging** check box.
- 7 Click **Update**.
If necessary, you can continue to configure additional settings by clicking the **Static Addresses**, **Aliases**, and **IPv6** tabs for the serial port connection. See “Configuring static IP addresses for a connection” on page 64, “Aliases tab” on page 43, and “Enabling IPv6 for a connection” on page 44.

Use this procedure to disable dial on demand for a connection. By default, the appliance continuously maintains the dialout connection.

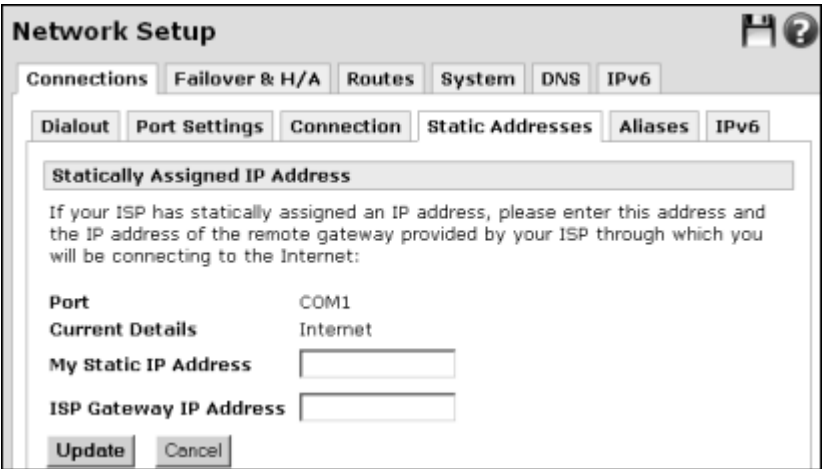
- 1 From the **Network Setup** menu, click **Network Setup**. The Connections page appears.
- 2 On the **Connections** page, click the **Edit** icon, then the **Connection** tab for the connection for which you want to disable dial on demand.
- 3 Clear the **Dial on Demand** check box.
- 4 Click **Update**.

Configuring static IP addresses for a connection

Use this procedure to configure a static IP Address for a connection. The majority of ISPs dynamically assign an IP address to your connection when you dial-in; however, some ISPs use pre-assigned static addresses.

- 1 From the **Network Setup** menu, click **Network Setup**. The **Connections** tab opens. Click the edit icon for the connection you want to edit.
- 2 Click the **Static Addresses** tab. The Statically Assigned IP Address page appears.

Figure 44: Port Settings
— Static Addresses



- 3 Enter the static IP address from your ISP in the **My Static IP Address** field.

- 4 Enter the address of the ISP gateway in the **ISP Gateway IP Address** field.
- 5 Click **Update**.

If necessary, you can continue to configure additional settings by clicking the **Aliases** and **IPv6** tabs for the serial port connection. See “Aliases tab” on page 43, and “Enabling IPv6 for a connection” on page 44.

Configuring interface aliases for a connection

Use this procedure to assign alias IP address for an Internet network connection. Alias addresses enable the appliance to accept incoming connections on the same TCP or UDP port for multiple servers. The alias addresses are in addition to the primary IP address assigned via the network connection configuration. You usually need to set up appropriate NAT Rules in order to make use of an alias address. These NAT rules can forward packets from the alias address to servers on the local network. For information, see “NAT” on page 245.

- 1 From the **Network Setup** menu, click **Network Setup**. The **Connections** tab opens. Click the edit icon for the connection you want to edit.
- 2 Click the **Aliases** tab. The Interface Aliases page appears.

Figure 45: Port Settings-
Alias tab — Interface
Aliases

The screenshot shows the 'Network Setup' window with the 'Aliases' tab selected. The 'Interface Aliases' section displays a table with one entry: 'iphouse' with 'Internet' details. Below the table, there are input fields for 'Alias IP Address' and 'Alias Subnet Mask' (currently set to 24). At the bottom are 'Add' and 'Cancel' buttons.

Alias IP Address	Alias Subnet Mask	Delete
123.45.45.6	24	

- 3 Enter the alias address in the **Alias IP Address** field.
 - 4 Enter the subnet mask for the alias in the **Alias Subnet Mask** field. The netmask can be either a number between 0 and 32, or in the form 255.255.255.0. The Alias Subnet Mask defaults to your current subnet mask.
 - 5 Click **Add**. The Aliased IP address is added to the edit list.
- If necessary, you can continue to configure additional settings by clicking the **IPv6** tab for the serial port connection. See “Enabling IPv6 for a connection” on page 44.

Setting up dial-in access

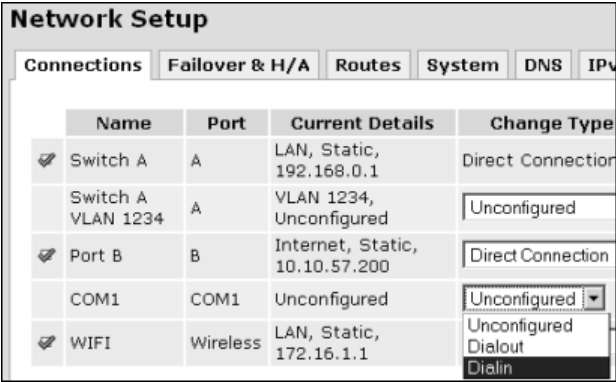
A remote user can dial directly to a modem connected to the serial port of the SnapGear appliance. Once connected and authenticated, the user has access to network resources as if they were a local user on the LAN. This is useful for remote administration of your appliance, or for telecommuting.

Note: Concurrent Dialin and Dialout configurations are not currently supported. Dialin access uses the PPP (Point-to-Point) protocol only. SLIP (Serial Line IP) and other protocols are not supported.

Dial-in setup

- 1 From the **Network Setup** menu, click **Network Setup**. The **Connections** tab opens.

Figure 46: Dial-in Change Type



- 2 From the **Change Type** list of the Connection you want to configure, select **Dialin**. The connection is the interface you want to connect to the dialup modem to answer incoming calls.

The Dial-In Setup Account Details page appears.

Figure 47: Dial-in Setup
tab — Account Details
page

The screenshot shows a web-based configuration interface titled "Network Setup". It has several tabs: "Connections", "Failover & H/A", "Routes", "System", "DNS", and "IPv6". The "Connections" tab is active, and within it, the "Dial-In Setup" sub-tab is selected. The "Account Details" section contains the following fields:

- Port:** COM1
- Current Details:** Unconfigured
- Connection Name:** An empty text input field.
- IP Address for Dial-In Clients:** An empty text input field.
- IP Address for Dial-In Server:** A dropdown menu currently showing "Switch A".
- Authentication Scheme:** A dropdown menu currently showing "Encrypted Authentication (MS-CHAP v2)".
- Required Encryption Level:** A dropdown menu currently showing "Strong Encryption (MPPE 128 Bit)".
- Authentication Database:** A dropdown menu currently showing "Local".

At the bottom of the form are two buttons: "Finish" and "Cancel".

- 3 [Optional] Enter a descriptive name for the connection in the **Connection Name** field.
- 4 In the **IP Address for Dial-In Clients** field, enter an available IP address. This IP address must not already be in use on the network (typically the LAN) that the remote user is assigned while connected to the SnapGear appliance.
- 5 If you have configured several network connections, select the one that you want to connect remote users to from the **IP Address for Dial-In Server** list. This is typically a LAN interface or alias.

- 6 Select the weakest Authentication Scheme to accept from the **Authentication Scheme** list. Access is denied to remote users who attempt to connect using an authentication scheme weaker than the selected scheme. Available schemes are:
 - **No Authentication**
 - **Unencrypted Authentication (PAP):** This is plain text password authentication. When using this type of authentication, the client passwords are transmitted unencrypted.
 - **Weakly Encrypted Authentication (CHAP):** This is the weakest type of encrypted password authentication to use. It is not recommended that clients connect using this as it provides very little password protection. Also note that clients connecting using CHAP are unable to encrypt traffic.
 - **Encrypted Authentication (MS-CHAP):** This is not a recommended encryption type and should only be used for older dial-in clients that do not support MS-CHAP v2.
 - **Encrypted Authentication (MS-CHAP v2):** [Recommended] The strongest type of authentication to use.
- 7 Select the encryption level from the **Required Encryption Level** list. Access is denied to remote users attempting to connect not using this encryption level. Available options are:
 - **No Encryption**
 - **Basic Encryption (MPPE 40 Bit)**
 - **Strong Encryption (MPPE 128 Bit)** Recommended.
- 8 Select the database used for authentication from the **Authentication Database** list. This allows you to indicate where the list of valid clients can be found. Available options are:
 - **Local:** Use the local database defined on the **Local Users** tab of the **Users** page. You must enable the **Dial-in Access** option for the individual users that are allowed dial-in access.
 - **RADIUS:** Use an external RADIUS server as defined on the RADIUS tab of the Users page.
 - **TACACS+:** Use an external TACACS+ server as defined on the TACACS+ tab of the Users page.

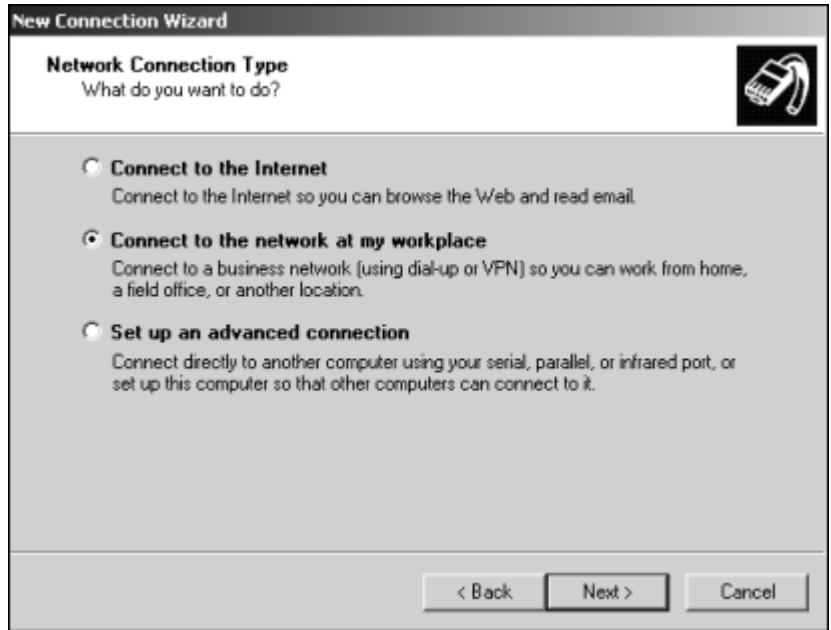
For details on adding user accounts for dial-in access, and configuring the SnapGear appliance to enable authentication against a RADIUS or TACACS+ server, see “Users menu” on page 476.
- 9 Click **Finish**. The Port Settings tab now becomes available. You can adjust settings if desired. Now configure the dial-in client. See the next procedure, “Connecting a dial-in client” on page 69.

Connecting a dial-in client

Remote users can dial in to the SnapGear appliance using the standard Windows **Dial-Up Networking** software. The network connection wizard guides you through setting up a remote access connection. The following instructions are for Windows XP.

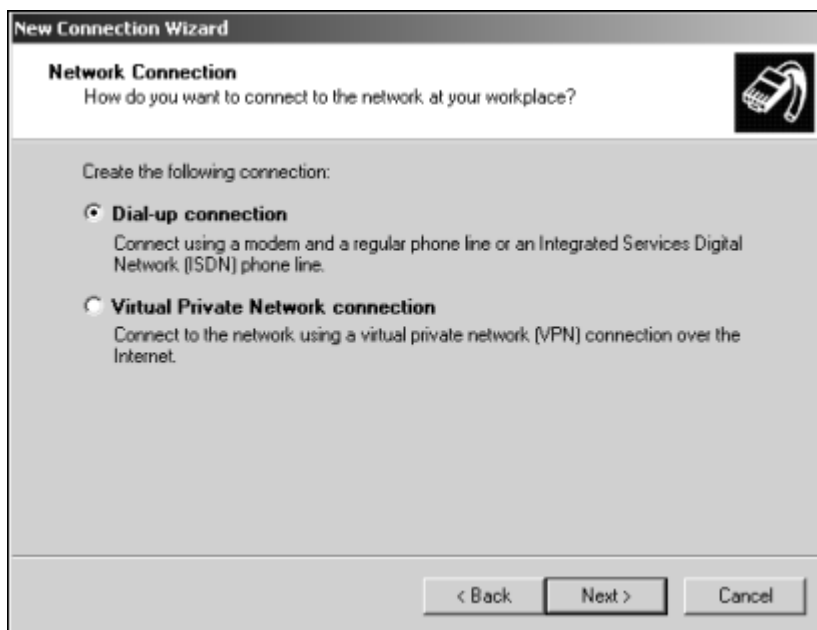
- 1 Click **Start > Settings > Network and Dial-up Connections** and select **Connect to the network at my workplace** option.

Figure 48: Network Connection Type



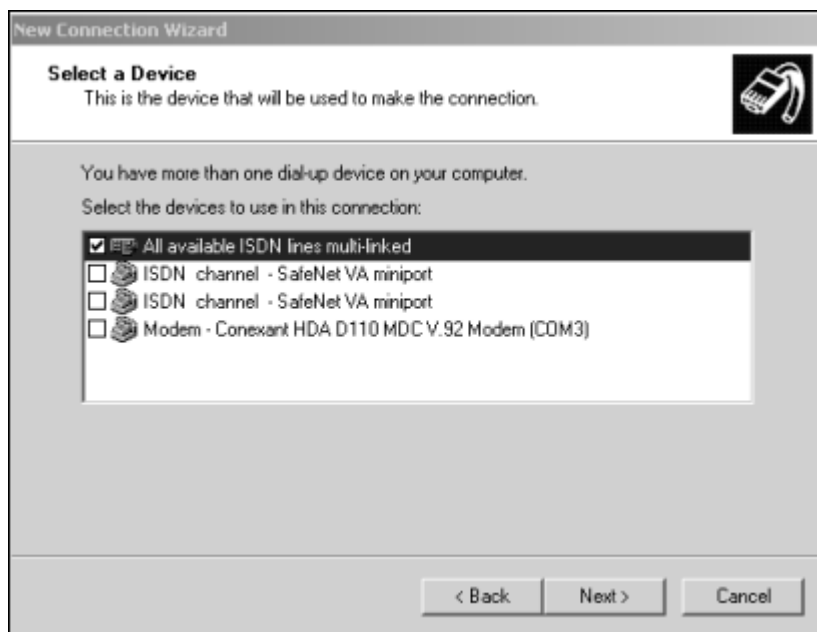
- 2 Click **Next** to continue.

Figure 49: Network Connection



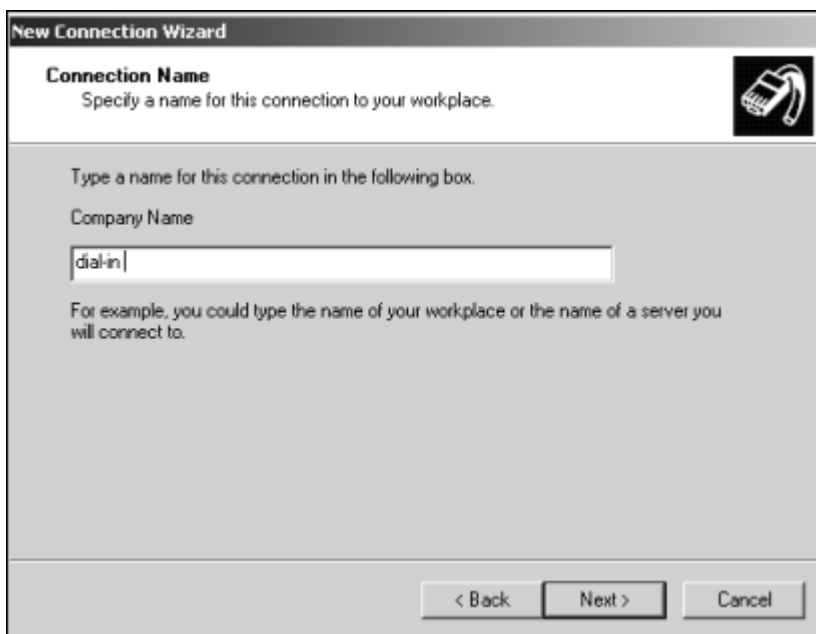
3 Select **Dial-up connection** and click **Next**.

Figure 50: Select Device



4 Select the device to use for the connection and click **Next**.

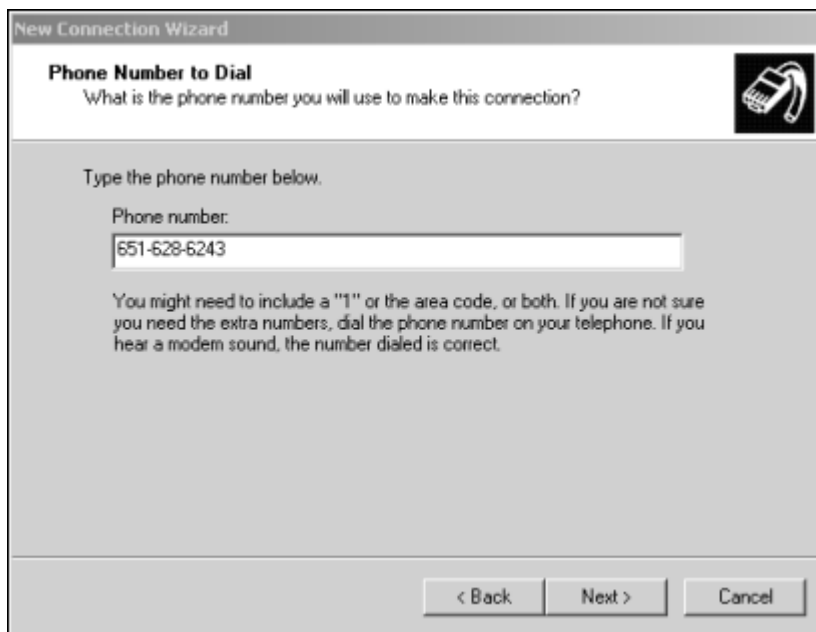
Figure 51: Connection Name



The screenshot shows the 'New Connection Wizard' window with the 'Connection Name' tab selected. The title bar reads 'New Connection Wizard'. Below the tab, the text says 'Specify a name for this connection to your workplace.' To the right is a modem icon. The main area contains the instruction 'Type a name for this connection in the following box.' followed by 'Company Name' and a text input field containing 'dial-in'. Below the field, it says 'For example, you could type the name of your workplace or the name of a server you will connect to.' At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

- 5 Enter a name for the connection and click **Next**.

Figure 52: Phone Number to Dial



The screenshot shows the 'New Connection Wizard' window with the 'Phone Number to Dial' tab selected. The title bar reads 'New Connection Wizard'. Below the tab, the text says 'What is the phone number you will use to make this connection?' To the right is a modem icon. The main area contains the instruction 'Type the phone number below.' followed by 'Phone number:' and a text input field containing '651-628-6243'. Below the field, it says 'You might need to include a "1" or the area code, or both. If you are not sure you need the extra numbers, dial the phone number on your telephone. If you hear a modem sound, the number dialed is correct.' At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

- 6 Enter the phone number to dial and click **Next**.

Figure 53: Smart Cards



- 7 Elect a smart card option and click **Next**.

Figure 54: Connection Availability



- 8 To make the connection only available for you, select the **My use only** option. This is a security feature that does not allow any other users who log onto your machine to use this remote access connection. Click **Next**.

Figure 55: Completion



- 9 To add an icon for the remote connection to the desktop, select the **Add a shortcut to this connection to my desktop** check box, and click **Finish**.

10 The Connect dial-in dialog box is displayed.

Figure 56: Connect dial-in



11 If you did not create a desktop icon, click **Start > Settings > Network and Dial-up Connections** and select the appropriate connection. Enter the **User name** and **Password** set up for the SnapGear appliance dial-in account and click **Dial**.

Failover, load balancing, and high availability

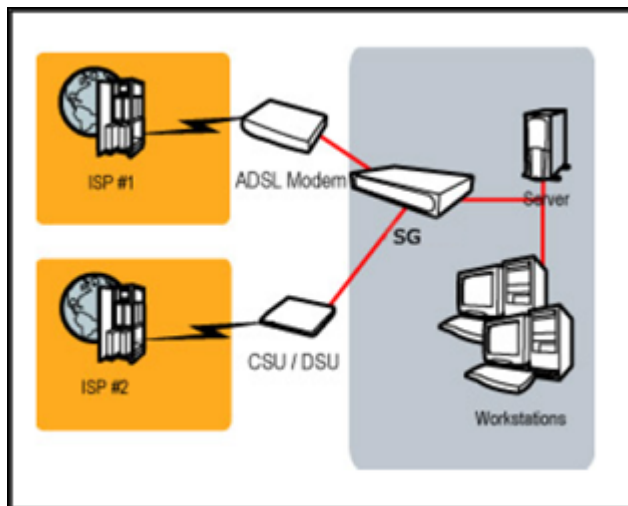
Note: This topic applies to SnapGear gateway (desktop) and rack mount appliances only. These features are not available for the PCI appliance.

The SnapGear appliance supports a wide range of configurations through which you can use multiple Internet connections, and even multiple SnapGear appliances, to ensure Internet availability in the event of service outage or heavy network load. These availability services can be configured individually or in combination. The following Internet availability services are provided by the SnapGear appliance:

- **Internet Connection Failover** — A backup, redundant Internet connection (or connections) that is only established should the primary link lose connectivity. See “Internet connection failover” on page 77.
- **Load Balancing** — Another Internet connection (or connections) concurrently with the primary link, for spreading network load over multiple connections. See “Load balancing” on page 83.
- **High Availability** — A backup, redundant SnapGear appliance to monitor the status of the primary appliance, coming online and becoming the Internet gateway for your network should the primary appliance fail. See “High Availability” on page 86.

The configuration shown in Figure 57 illustrates a SnapGear appliance that connects via an ADSL modem and a CSU/DSU (Channel Service Unit/Data Service Unit required for T1 and T3 lines) to two different ISPs (Internet Service Providers):

Figure 57: Failover, load balancing, and high availability configuration



Note: *The SnapGear model SG300 is limited to Internet availability configurations using a single broadband Internet connection and a single dialout or ISDN connection.*

Configure all Internet connections to use in conjunction with the Internet availability services. Secondary and tertiary Internet connections are configured in the same manner as the primary Internet connection, as detailed in the sections Direction Connection, ADSL, Cable Modem, and Dialout/ISDN earlier in this chapter. See “Direct connection overview” on page 38, “ADSL” on page 46, “Connecting with a cable modem” on page 55, and “Configuring a dialout connection on the COM port” on page 59. Once the Internet connections have been configured, specify the conditions under which the Internet connections are established.

If you are using a SnapGear model SG560, SG565, or SG580, you might want to skip to information on establishing multiple broadband connections. See “Port-Based VLANs” on page 129.



Important: *If you have configured the switch of your SG560, SG565, or SG580 as separate ports, and are establishing multiple PPPoE ADSL Internet connections using two or more of these ports, it is important that each port A is connected to a remote device (DSLAM) with a unique MAC address, since the DSLAM may use the same MAC address for all DSL connections. Duplicate MAC address issues are still possible even if each of the Internet connections are through different ISPs, as often multiple ISPs share the same DSLAM. If your ISPs are unable to correct the issue, set the second and subsequent ADSL modems connected to the A port switch to routing or NAT rather than bridged mode to hide the duplicate MAC address from the SnapGear appliance. Typically, this means the ADSL modem terminates the PPPoE connection, and the appliance is configured with DHCP or manually assigned settings, using the ADSL modem as a gateway.*

Internet connection failover

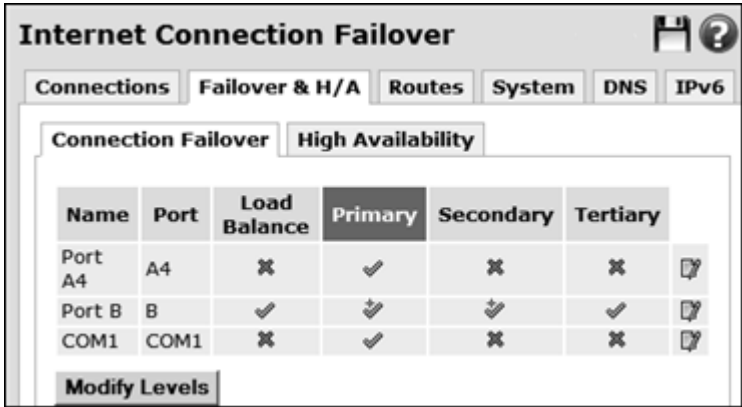
SnapGear appliances support three connection levels: Primary, Secondary, and Tertiary. A *connection level* consists of one or more Internet connections. When all primary connections are functioning as expected, the primary connection level is deemed to be up. If one or more of the primary connections should fail, the appliance drops back to the secondary connection level. This typically involves bringing up a secondary Internet connection until the primary Internet connection or connections become available again. A scenario where secondary and tertiary levels are particularly useful is when multiple connections share the same public IP address, and only one connection at a time is desired to be active at any given time. You can also optionally configure the tertiary failover level. If one or more of the secondary connections should fail, the appliance drops back to the tertiary connection level. This is typically a last resort dialup link to the Internet, but can be any kind of network connection. The primary and secondary connection levels are tested in turn until one becomes available. Internet failover is not stateful. Any network connections that were established through the failed primary connection must be re-established through the secondary connection.

Editing failover connection parameters

The initial step of configuring failover is to set failover parameters for each connection. These parameters specify how to test whether a connection is up and functioning correctly. Then you modify the failover levels.

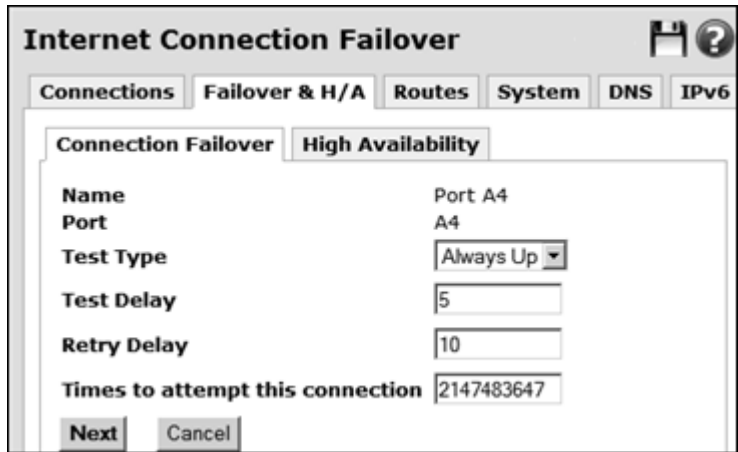
- 1 From the **Network Setup** menu, click **Network Setup**. The Connections page appears.
- 2 Click the **Failover & H/A** tab. A list of the connections that you have configured is displayed under the **Connection Failover** tab, alongside ticks (check marks) and cross marks. The ticks and crosses indicate how the connection behaves at each failover level:
 - **Enabled** — Check mark (tick)
 - **Required** — Check mark with a small plus sign
 - **Disabled** — Cross mark.

Figure 58: Connection
Failover



- 3 Click the **Edit** icon next to the connection to edit its failover parameters. The edit page for failover parameters appears. The **Name** and **Port** of the connection is displayed, along with several connection testing options.

Figure 59: Connection
Failover Name and Port



- 4 Select a **Test Type**. The **Ping** test is usually appropriate. Available options are:
- **Always Up** — Disables Internet failover for this connection. No connection testing is performed.
 - **Ping** — Sends network traffic to a remote host at regular intervals, if a reply is received, the connection is deemed to be up.
 - **Custom** (*advanced users only*) — Allows you to enter a custom console command to run to determine whether the connection is up. This is typically a script you have written and uploaded to the SnapGear appliance.

You can adjust the timeouts for the failover test; however, the defaults are usually suitable.

- 5 In the **Test Delay** field, enter the number of seconds to wait after starting this connection before testing whether it is functioning correctly. Use a longer delay for connection types that are slow to establish, such as dialout. The defaults vary depending on the type of connection, and are as follows:
 - 5 (direct connection)
 - 10 (PPTP/PPPoE connection)
- 6 In the **Retry Delay** field, enter the number of seconds to wait after a connection test fails before attempting the test again. The defaults vary depending on the type of connection, and are as follows:
 - 5 (direct connection)
 - 30 (PPTP/PPPoE connection)
- 7 In the **Times to attempt this connection** field, enter the number of times to try a connection. Once the SnapGear appliance has ceased testing this connection, manual intervention is required to re-establish the connection.
 - Default: 2147483647
- 8 Click **Next** to configure settings specific to the **Test Type**.
 - If you selected a **Test Type** of **Always Up**, no further configuration is required. Click **Finish**. The next step is to modify the failover levels. See “Modifying failover levels” on page 81.

Figure 60: Always Up mode



- If you selected **Custom**, the page to enter a custom test command appears:

Figure 61: Custom Test Command

The screenshot shows the 'Internet Connection Failover' dialog box with the 'Custom Test Command' tab selected. The 'Test Command' field is empty. The 'Back', 'Finish', and 'Cancel' buttons are at the bottom.

- Enter the custom command to test the connection in the **Test Command** field. An example script is as follows:

```
myscript 5 10 ping -c 1 -I $if_netdev 15.1.2.3
```

Replace *\$if_netdev* with the name of the network interface on which you are running the test, such as **ppp0**.

- Click **Finish**. If the **Test Command** exits with a return code of zero (0), the connection passed the test and is considered up; otherwise, the connection is considered down.

The next step is to modify the failover levels. See “Modifying failover levels” on page 81.

- If you selected **Ping**, the page to enter Ping test details appears:

Figure 62: Ping command

The screenshot shows the 'Internet Connection Failover' dialog box with the 'Ping test details' tab selected. The fields are: 'IP address to ping' (0.0.0.0), 'Ping interval' (10), and 'Failed pings until down' (5). The 'Back', 'Finish', and 'Cancel' buttons are at the bottom.

- Enter an address in the **IP Address to Ping** field. Choose a host on the Internet that responds to pings and can be reliably contacted. You can check whether you can ping a host under **Diagnostics > Network Tests > Ping Test**. For details, see “Network Tests page” on page 503.

- Can be a fully qualified domain name of the form *host.domain.com*. Both *Host* or *domain* can consist of alphabetic, numeric, or hyphen (-) characters, but cannot begin nor end with the hyphen character.
 - Can be an IP address of the form *a.b.c.d*
- b** Enter the time in seconds to wait between sending each ping in the **Ping interval** field.
- Default: 10
 - Can be zero (0) or greater
- c** In the **Failed pings until down** field, enter the number of missed ping replies before this connection attempt is deemed to have failed.
- Default: 5
- d** Click **Finish**. The next step is to modify the failover levels. See “Modifying failover levels” on page 81.

Modifying failover levels

The next step of configuring Internet failover is associating Internet connections with primary, secondary, and optionally tertiary connection levels. Recall that a connection level is one or more connections. These connections must be marked as **Required** or **Enabled**. Internet connections that are marked **Disabled** are not part of this connection level. The initial defaults on the modify levels page for a connection are:

- Load balancing — Disabled
- Primary — Enabled
- Secondary — Enabled
- Tertiary — Enabled

A connection level is deemed to be up when all connections marked **Required** at that level are up, and at least one connection marked **Required** or **Enabled** at that level is also up.

- 1 From the **Network Setup** menu, click **Network Setup > Failover & H/A tab > Modify Levels**. A table is displayed listing each of the connections alongside a list for each connection level.

Figure 63: Connection
Failover Modify Levels

Name	Port	Load Balance	Primary	Secondary	Tertiary
A3 port	A3	<input checked="" type="checkbox"/>	Enabled	Disabled	Disabled
Port B	B	<input checked="" type="checkbox"/>	Required	Required	Enabled
test dialout	COM1	<input type="checkbox"/>	Enabled	Disabled	Disabled

- 2 First, configure the Primary connection level by selecting an option from the **Primary** list. If you only have a single Internet connection, setting the level to **Enabled** or **Required** has the same effect.
- 3 For failover to succeed, you must then configure at least the Secondary connection level for another port or ports. Select **Enabled** or **Required** from the **Secondary** list.
- 4 [Optional] Select a **Tertiary** failover for yet another port or ports.
- 5 [Optional] Select the **Load Balance** check box to enable load balancing for two or more ports. For more information, see “Load balancing” on page 83.
- 6 Click **Finish**.

Load balancing

Once you have configured two or more Internet connections, you can enable Internet load balancing. Load balancing can be used in conjunction with Internet connection failover or on its own to specify the connection as the preferred default route.

Load balancing settings are not specified for each failover level; load balancing occurs when any two or more load balancing connections are up. The Internet connections need not be the same; for example, you can enable load balancing between a PPPoE ADSL connection on one network port, and a Cable Internet connection on the other.

Limitations of load balancing

Load balancing works by alternating outgoing traffic across Internet connections in a round-robin manner. It does not bond both connections together to work as one link; that is, it does not bond two 512 Kbit/s links to function as a single 1 Mbit/s link. Total bandwidth and available bandwidth are not taken into account when choosing a connection on which to send outgoing traffic.

When an internal client makes a connection to a server on the Internet, this and subsequent connections between the internal client and remote server are confined to the one Internet connection to ensure connections are not broken. If a second internal client makes a connection to the same remote server, it may or may not go across the same link, depending on which Internet connection is selected next in the process. VPN connections such as IPSec or PPTP tunnels are confined to a single Internet connection, as they are a single connection that encapsulates other connections.

Load balancing is not performed for incoming traffic. This scenario can be addressed using other solutions such as round-robin DNS to alternate incoming connections between the two links.

Enabling load balancing

Use this procedure to enable load balancing. You can configure load balancing for any configured Internet connection. All active Internet connections with load balancing enabled become the preferred default route. If only one Internet connection is enabled, it becomes the preferred default route. If two or more connections are enabled for load balancing, traffic is balanced equally across those connections.

- 1 From the **Network Setup** menu, click **Network Setup > Failover & H/A** tab. The Internet Connection Failover page appears.

Figure 64: Connection Failover page

Name	Port	Load Balance	Primary	Secondary	Tertiary
Port B	B	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
COM1	COM1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- 2 Click **Modify Levels**. A table is displayed listing each of the connections alongside a list for each connection level.

Figure 65: Load balancing

Name	Port	Load Balance	Primary	Secondary	Tertiary
A3 port	A3	<input checked="" type="checkbox"/>	Enabled	Disabled	Disabled
Port B	B	<input checked="" type="checkbox"/>	Required	Required	Enabled
test dialout	COM1	<input type="checkbox"/>	Enabled	Disabled	Disabled

- 3 Select the **Load Balance** check box for each connection you want to enable load balancing for.

Note: Each connection you are load balancing must have at least one level (Primary, Secondary, Tertiary) enabled.

- 4 Click **Finish**. The Connection Failover page shows load balancing for a connection as either enabled (check mark) or disabled (cross mark).

Figure 66: Load balancing status

The screenshot shows the 'Internet Connection Failover' window with the 'Connection Failover' tab selected. The 'High Availability' sub-tab is also active. A table displays the status of three connections: 'A3 port', 'Port B', and 'test dialout'. Each row shows the connection name, port, load balance status, and primary, secondary, and tertiary failover status. Checkmarks indicate enabled status, while crosses indicate disabled status. A 'Modify Levels' button is located at the bottom left of the table area.

Name	Port	Load Balance	Primary	Secondary	Tertiary
A3 port	A3	✓	✓	✗	✗
Port B	B	✓	✓	✓	✓
test dialout	COM1	✗	✓	✗	✗

Modify Levels

High Availability

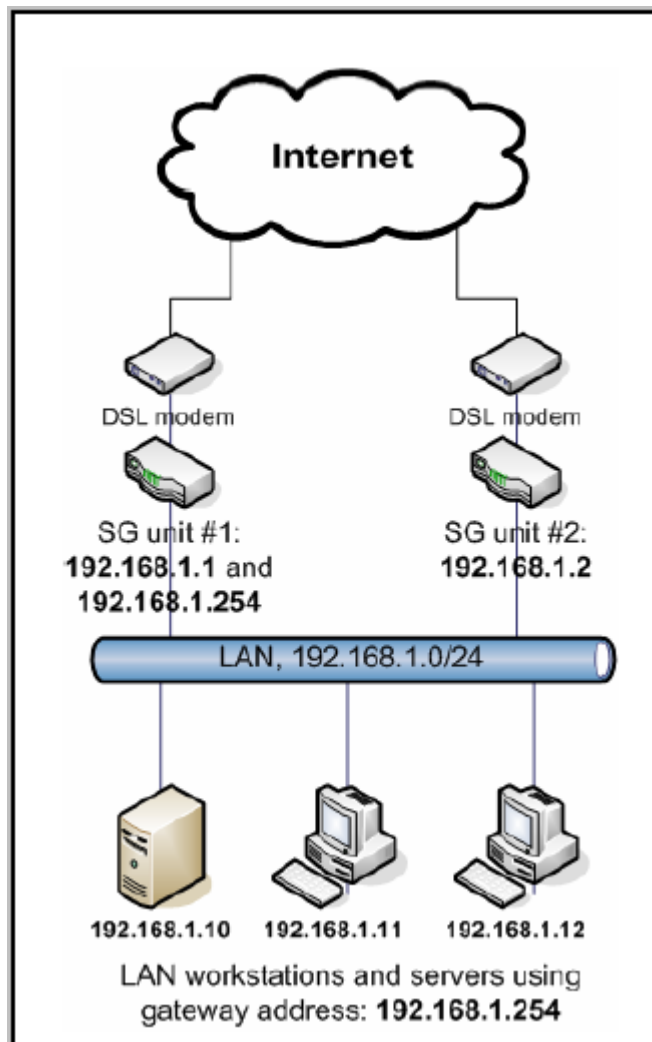
High Availability (HA) allows a second SnapGear appliance to provide network connectivity should the primary SnapGear appliance fail. The SnapGear appliances do not have to be the same models to be used in the HA pair. If you have two SnapGear appliances on the same network segment, you can configure a shared IP address that is assigned to one or the other appliance (as an Ethernet alias address) depending upon which appliance is available. This provides for simple high availability support, which is useful when hosts on the LAN segment have their default gateway assigned as the shared IP address. This allows these hosts to automatically switch from one SnapGear appliance to the other if an appliance becomes unavailable. The two appliances negotiate for ownership of the shared IP address at any given time. The appliance that currently has the address is termed the *master* or *primary* appliance while the other device is termed the *slave* or *secondary* appliance.

A shared IP address, such as 192.168.1.254, is automatically configured as an alias on the interface on that network segment on one of the SnapGear appliances. This is done via simple negotiation between the two SnapGear appliances such that one appliance has the IP address (the primary appliance) and one does not (the secondary appliance). This shared IP address is in addition to the primary IP addresses of the two SnapGear appliances (for example, 192.168.1.1 and 192.168.1.2) for the interface on the network segment. The shared IP address and primary IP addresses of the two SnapGear appliances are usually part of the same network (for example, 192.168.1.0/24), but need not be. Typically, hosts on the local network use the shared IP address as their gateway, and only use the devices' primary IP addresses when they need to contact a particular SnapGear appliance, such as to access the Web management console of that appliance.

It is also possible to switch multiple network interfaces with high availability. In this case, one of the interfaces is designated as the *checking* interface. You can specify additional interfaces that are also switched. When the appliance becomes master, all specified interfaces will have the appropriate shared IP address assigned. When the appliance becomes slave, all specified interfaces will have the shared IP address removed.

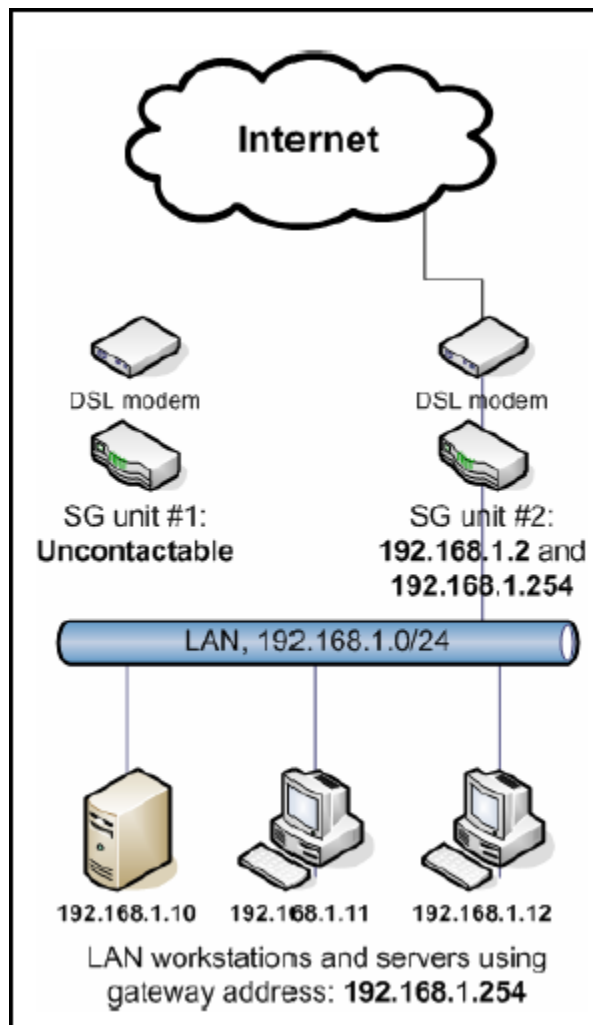
The following diagrams illustrate the basic HA configuration:

Figure 67: Basic HA configuration



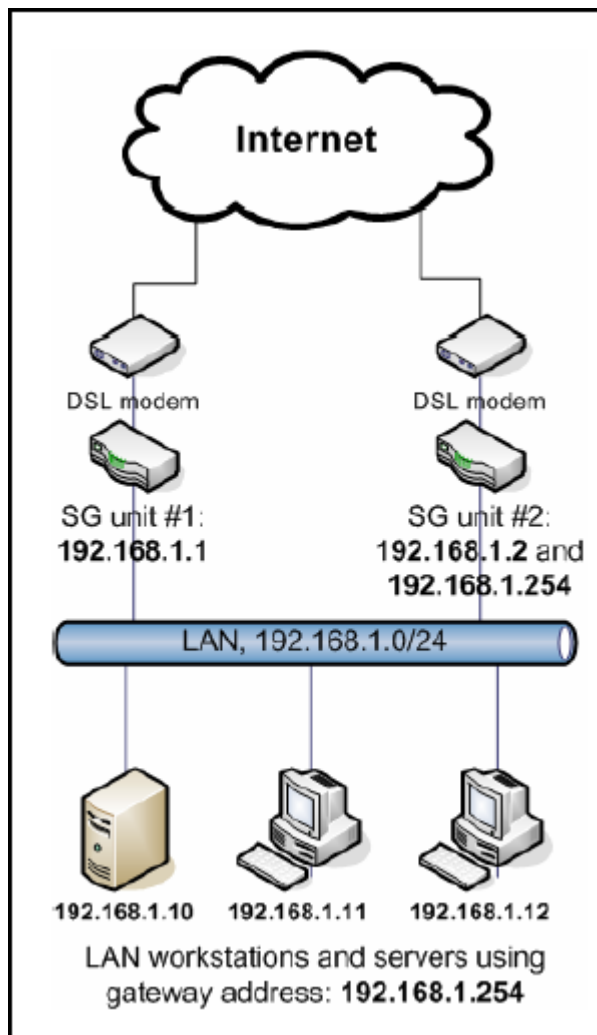
In the scenario illustrated in Figure 67, SnapGear appliance #1 is initially the primary (master) appliance and therefore the default gateway for the local network. SnapGear appliance #2 is the secondary appliance on standby. The standby status could be due to SnapGear appliance #1 booting up before SnapGear appliance #2, or SnapGear appliance #2 might have previously failed but has come back online.

Figure 68: Basic HA configuration: Appliance 1 loses LAN connectivity



Should SnapGear appliance #1 lose LAN connectivity (for example, someone accidentally powers it down), SnapGear appliance #2 assumes the shared IP address and becomes the default gateway for the local network, as illustrated in Figure 68.

Figure 69: Basic HA configuration—Appliance 1 gains LAN connectivity



Later, SnapGear appliance #1 comes back online as the secondary (slave). SnapGear appliance #2 continues its role as the default gateway for the local network.

Default high availability script

With the default high availability script, a high availability failover is not triggered by the primary simply losing Internet connectivity. The primary must become uncontactable to the secondary via the local network segment in order for an HA failover to trigger. The default location for the HA script is */bin/highavaild*.

Customizing the HA script

You can customize the HA script by replacing and modifying the */bin/highavaild* script. From the command line interface, (ssh/telnet) copy */bin/highavaild* to */etc/config*. Edit the HA script with *vi* or via the Web management console System menu Advanced option (see “Configuration Files tab” on page 519). You must also change the HA path for *highavaild* to */etc/config/highavaild*. See “Enabling high availability” on page 91.

The share-IP address will automatically be configured as an alias interface by the HA script and logic on whichever appliance is currently the primary (master). More sophisticated HA scenarios can be configured by setting up a basic configuration in the High Availability page and then manually editing the *ifmond.conf* file and the scripts it calls.

Enabling high availability

- 1 From the **Network Setup** menu, click **Network Setup > Failover & H/A > High Availability** tab.

Figure 70: High Availability page

The screenshot shows a web-based configuration interface titled "High Availability". At the top, there are tabs for "Connections", "Failover & H/A", "Routes", "System", "DNS", and "IPv6". Under the "Failover & H/A" tab, there are sub-tabs for "Connection Failover" and "High Availability", with the latter being selected. The "High Availability" section contains a checkbox labeled "Enable High Availability" which is checked. Below it is a text field for "High Availability Script Pathname" containing the value "/bin/highavaild". A "Submit" button is located below the text field. At the bottom of the section, there are buttons for "Check", "Network Interface", "IP Address", and "Subnet Mask". Below these buttons, the text "No entries" is displayed. A "New" button is located at the bottom left of the form.

- 2 Select the **Enable High Availability** check box.
- 3 [Optional] If you are customizing the script for high availability, change the HA path from `/bin/highavaild` to `/etc/config/highavaild`. For further details, refer to "Customizing the HA script" on page 90.
- 4 Click **Submit**. An action successful message is displayed. You can now configure the HA connection for each interface. See "Configuring high availability" on page 92.

Disabling high availability

- 1 From the **Network Setup** menu, click **Network Setup > Failover & H/A > High Availability** tab.
- 2 Clear the **Enable High Availability** check box.
- 3 Click **Submit**. An action successful message is displayed.

Configuring high availability

Use this procedure to configure high availability for an interface.



Important: Both SnapGear appliances must have an identical HA configuration, including the list of interfaces, shared IP addresses, and the interface configured as the checked interface.

- 1 From the **Network Setup** menu, click **Network Setup > Failover & H/A > High Availability** tab.
- 2 Click **New**. The Edit High Availability Connection page appears.

Figure 71: High Availability

- 3 Select the **Check this interface** check box.
- 4 Select the interface to check for high availability from the **Network Interface** list.
- 5 Enter the shared IP address in the **IP Address** field. The address can be of the form:

- *a.b.c.d*

Note: The HA shared IP address is treated the same as an alias. VPN connections are accepted; however, administration connections are not.

- 6 Enter the netmask in the **Subnet Mask** field. Can be in the following forms:
 - A number from 0-32
 - 255.255.255.0
- 7 Click **Finish**. The connection is added to the edit list.

Figure 72: HA connections

High Availability

Connections Failover & H/A Routes System DNS IPv6

Connection Failover High Availability

Enable High Availability ☒

High Availability Script Pathname

Submit

Check	Network Interface	IP Address	Subnet Mask		
<input type="checkbox"/>	Switch A	0.0.0.0	24		
<input type="checkbox"/>	Port A2	3.3.3.3	24		
<input checked="" type="checkbox"/>	Wireless	3.3.3.3	24		

New

- 8 Repeat this procedure for the secondary appliance.

DMZ network

Note: DMZ is not available on the SG300 or SG640 PCI appliances.

A DMZ (de-militarized zone) is a physically separate LAN segment, typically used to host servers that are publicly accessible from the Internet. Servers on this segment are isolated to provide better security for your LAN. If an attacker compromises a server on the LAN, then the attacker immediately has direct access to your LAN. However, if an attacker compromises a server in a DMZ, they are only able to access other machines on the DMZ.

By default, the SnapGear appliance blocks network traffic originating from the DMZ from entering the LAN. Additionally, any network traffic originating from the Internet is blocked from entering the DMZ and must be specifically allowed before the servers become publicly accessible. However, network traffic originating from the LAN is allowed into the DMZ and network traffic originating from the DMZ is allowed out to the Internet.

The topic “Services on the DMZ network” on page 96 discusses how to allow certain traffic from the Internet into the DMZ. To allow public access to the servers in the DMZ from the Internet, this step must be performed. You can also allow certain network traffic originating from the DMZ into the LAN; however, this is not usually necessary.

By default, the SnapGear configuration expects machines on the DMZ network to have addresses in a private IP address range; for example, *192.168.1.0 / 255.255.255.0* or *10.1.0.0 / 255.255.0.0*. Real world addresses can be used on the DMZ network by clearing the **Enable NAT from DMZ interfaces to Internet interfaces** check box under the Advanced tab, which enables routing to the DMZ public addresses. You also need to ensure that upstream routers are aware of this routing configuration, typically by communicating with your ISP. For further information, see “NAT” on page 245.

Configuring a DMZ connection

- 1 From the **Network Setup** menu, click **Network Setup > Connections** tab. The Connections page appears.
- 2 For the network port being connected to the DMZ, select **Direct Connection** from the **Change Type** list. The Direct Connection Settings page appears.

Figure 73: Direct DMZ Connection

The screenshot shows the 'Network Setup' window with the 'Connections' tab selected. Under 'Direct Connection', the 'Direct Connection Settings' sub-tab is active. The settings are as follows:

Field	Value
Port	A4
Current Details	VLAN 3, DMZ, DHCP
Connection Name	DMZ_Port_A4
DHCP assigned	<input checked="" type="checkbox"/>
IP Address	
Subnet Mask	24
Gateway	
DNS Server(s)	
Firewall Class	DMZ

Buttons: Update, Cancel

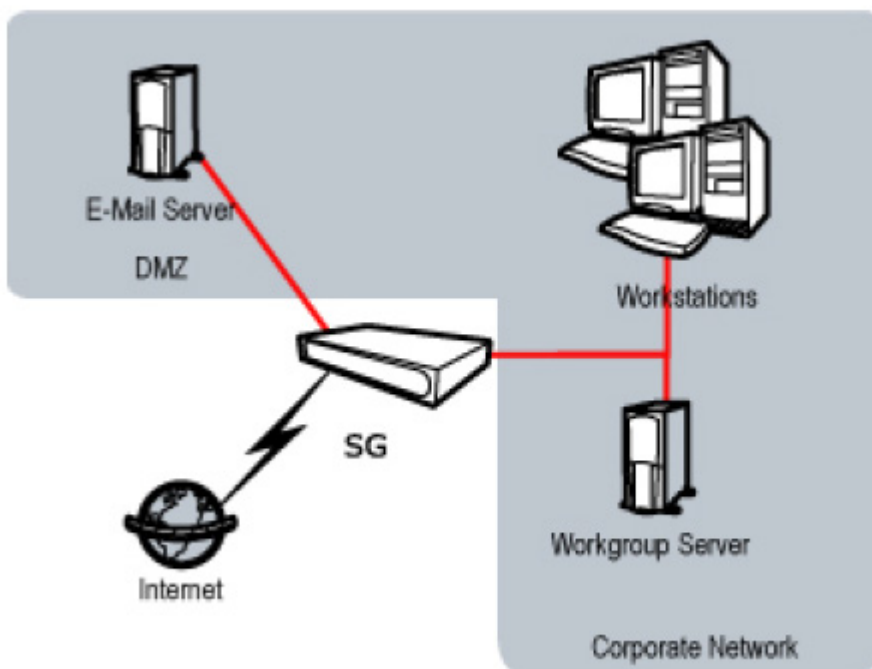
- 3 Enter a descriptive name for the connection, such as **DMZ_Port_A4**, in the **Connection Name** field.
- 4 Indicate the IP Address:
 - If the interface uses DHCP for IP assignment, select the **DHCP assigned** check box.
 - If DHCP is not being used, enter the appropriate IP Address in the **IP Address** field and the appropriate Subnet Mask in the **Subnet Mask** field.
- 5 If the default gateway is via the DMZ, enter the IP Address of the gateway in the **Gateway** field.
- 6 Define the DNS server the appliance uses for DNS resolution in the **DNS Server** field. Separate multiple entries with a comma or space.
- 7 Select **DMZ** from **Firewall Class** list.
- 8 Click **Update**.

Services on the DMZ network

Once you have configured the DMZ connection, configure the SnapGear appliance to allow access to services on the DMZ. There are two methods of allowing access:

- If the servers on the DMZ have public IP addresses, you need to add packet filtering rules to allow access to the services. For more information, see “Packet Filter Rules page” on page 232.
- If the servers on the DMZ have private IP addresses, you need to port forward the services. For further information, see “About port forwarding” on page 245. Creating port forwarding rules automatically creates associated packet filtering rules to allow access. However, you can also create custom packet filtering rules if you want to restrict access to the services.

Figure 74: DMZ sample network



You may also want to configure your appliance to allow access from servers on your DMZ to servers on your LAN. By default, all network traffic from the DMZ to the LAN is dropped.

Guest network

Note: Guest network is not available on the SG300 or SG640 PCI appliances.

The intended usage of guest connections is for connecting to a guest network, which is an untrusted LAN or wireless network. Machines connected to the guest network must establish a VPN connection to the SnapGear appliance in order to access the LAN, DMZ, or Internet. Once a VPN connection is established over a guest interface, access is allowed to all other firewall classes by default through the VPN connection.

By default, you can configure the appliance's DHCP server to hand out addresses on a guest network, and the appliance's VPN servers to listen for connections from a guest network and establish VPNs. Aside from this, access to any LAN, DMZ, or Internet connections from the guest network is blocked.

If you want to allow machines on a guest network direct access to the Internet, LAN, or DMZ without first establishing a VPN connection, add packet filtering rules to allow access to services on the LAN or Internet as desired.



Caution: Caution is advised before allowing machines on a guest network direct access to your LAN, which may make it easier for an attacker to compromise internal servers. Caution is also advised before allowing machines on a guest network direct access to the Internet, particularly in the case of guest wireless networks. This may result in unauthorized use of your Internet connection for sending spam, other malicious or illegal activities, or simply Internet access at your expense.

Machines on the guest network typically have addresses in a private IP address range, such as 192.168.2.0 / 255.255.255.0 or 10.2.0.0 / 255.255.0.0. For NAT (Network Address Translation) purposes, the guest connection is considered a LAN interface. In the Masquerading page, the **Enable NAT from LAN/VPN to Internet or DMZ** check boxes also apply to a guest connection. See the "NAT" on page 245 and "About masquerading and source NAT" on page 246 for further information.

Configuring a guest connection

Use this procedure to configure a guest connection, which is based on configuring a direct connection. Configuring a direct Connection is described in detail in “Direct connection overview” on page 38.

- 1 From the **Network Setup** menu, click **Network Setup**. The Connections page appears.
- 2 Select **Direct Connection** from the **Configuration** list of the network port you want to connect to the guest network. The Direct Connection Settings page appears.
- 3 [Optional] Enter a name for the connection, such as **Guest**, in the **Connection Name** field.
- 4 Indicate the IP Address:
 - If the interface uses DHCP for IP assignment, select the **DHCP assigned** check box.
 - If DHCP is not being used, enter the appropriate IP Address in the **IP Address** field and the appropriate Subnet Mask in the **Subnet Mask** field.
- 5 Select **Guest** from **Firewall Class** list.
- 6 Click **Update**. An action successful message is displayed. To view the guest connection on the Connections page, click the uppermost **Connections** tab.

Figure 75: Guest Connection

The screenshot shows the 'Network Setup' window with the 'Connections' tab selected. Under the 'Direct Connection' sub-tab, the 'Direct Connection Settings' section is visible. The settings are as follows:

Field	Value
Port	A4
Current Details	VLAN 3, Guest, DHCP
Connection Name	Guest
DHCP assigned	<input checked="" type="checkbox"/>
IP Address	
Subnet Mask	24
Gateway	
DNS Server(s)	
Firewall Class	Guest

At the bottom of the settings section are two buttons: 'Update' and 'Cancel'.

Wireless

Note: *Wireless is applicable to the SG565 model only.*

The SnapGear appliance's wireless interface can be configured as a wireless access point, accepting connections from 802.11b (11 Mbit/s)- or 802.11g (54 Mbit/s)-capable wireless clients.

Typically, the appliance's wireless interface is configured in one of two ways; with strong wireless security (WPA) to bridge wireless clients directly onto your LAN, or with weak wireless security as a Guest connection. The latter requires wireless clients to establish a VPN tunnel on top of the wireless connection to access the LAN, DMZ, and Internet to compensate for the security vulnerabilities WEP poses.

In addition to connection configuration, you can also configure wireless access point, access control list (ACL), and advanced settings.

Tip: *You can also opt to select the **Access Point** option from the **Change Type** list, which automatically creates a bridge to the LAN. See "Bridging wireless and LAN connections" on page 108.*

Wireless security methods

The following wireless security methods are supported:

- **None** — Any client is allowed to connect, and there is no data encryption.
- **WEP (Wired Equivalent Privacy)** — Allows for 64- or 128-bit encryption.
- **WEP with 802.1X** — Extends WEP to use the IEEE 802.1X protocol to authenticate the user and dynamically assign a 128-bit encryption key via a RADIUS server. This is a significant improvement to the security of WEP. The RADIUS server must be defined on the RADIUS page. For information, refer to "RADIUS page" on page 483.
- **WPA-PSK (Wi-Fi Protected Access Preshared Key, also known as WPA-Personal)** — An authentication and encryption protocol that fixes the security flaws in WEP. This security method is recommended if you do not have a RADIUS server. If you elect to use the AES encryption protocol with WPA-PSK, then this method is also known as WPA2 or 802.11i.



Security Alert: *If you use WEP or no wireless security method at all, Secure Computing highly recommends you configure the wireless interface as a Guest connection, disable bridging between clients, and only allow VPN traffic over the wireless connection.*

This section contains the following procedures:

- "Configuring a wireless connection"
- "Bridging wireless and LAN connections" on page 108
- "Configuring Wireless MAC-based ACL" on page 110
- "Configuring WDS" on page 113
- "Configuring advanced wireless features" on page 116

Configuring a wireless connection

Use this procedure to configure a wireless connection.



Security Alert: Secure Computing strongly recommends configuring the wireless interface as a LAN connection only if wireless clients are using WPA-based encryption/authentication. For more information, see WPA-PSK and WPA-Enterprise in "Wireless security methods" on page 99.

- 1 From the **Network Setup** menu, click **Network Setup**. The Connections page appears.
- 2 Select **Direct Connection** from the **Change Type** list of the wireless network interface.

Figure 76: Direct Connection for Wireless

Network Setup

Connections

Failover & H/A

Routes

System

DNS

IPv6

Name	Port	Current Details	Change Type
Switch A	A	LAN, Static, 192.168.0.1	Direct Connection
Port B	B	Unconfigured	Unconfigured
Wireless	Wireless	Unconfigured	Unconfigured
COM1	COM1	Unconfigured	Unconfigured Access Point Direct Connection

- 3 The Direct Connections Settings page appears.

Figure 77: Direct Connection for Wireless

The screenshot shows the 'Network Setup' window with the 'Connections' tab selected. Under the 'Direct Connection' sub-tab, the 'Direct Connection Settings' section is visible. The settings are as follows:

Direct Connection Settings	
Port	Wireless
Current Details	Unconfigured
Connection Name	<input type="text"/>
DHCP assigned	<input type="checkbox"/>
IP Address	<input type="text"/>
Subnet Mask	<input type="text" value="24"/>
Gateway	<input type="text"/>
DNS Server(s)	<input type="text"/>
Firewall Class	Guest <input type="button" value="v"/>

At the bottom of the settings section are three buttons: 'Back', 'Next', and 'Cancel'.

Note: Configuring a **Direct Connection** is described in detail in “Direct Connection Settings page” on page 38.

- 4 Enter appropriate IP address information for the wireless network.
- 5 From the **Firewall Class** list, select whether your wireless network is a **Guest**, **DMZ**, **LAN** or **Internet** connection.

Note: See the sections “Configuring a DMZ connection” on page 95 and “Configuring a guest connection” on page 98 for further information about DMZ and Guest network types.

- 6 Click **Next**. The Access Point Configuration page appears.

Figure 78: Wireless
Configuration — Access
Point page

The screenshot shows the 'Network Setup' window with the 'Wireless Configuration' tab selected. Under the 'Access Point Configuration' sub-tab, the following settings are visible:

- MAC Address: 00:0E:8E:01:06:CF
- ESSID: Test
- Broadcast ESSID: ☒
- Channel/Frequency: 1 / 2412 MHz
- Bridge Between Clients: ☐
- Security Method: WPA-PSK
- WPA Encryption: TKIP
- WPA Key: abcd1234

At the bottom of the configuration area are 'Finish' and 'Cancel' buttons.

- 7 [Optional] Enter a descriptive name for the wireless network in the **ESSID** field. The ESSID (Extended Service Set Identifier) is a unique name that identifies a wireless network. The field attributes are as follows:
 - Case-sensitive
 - 1-32 alphanumeric characters
- 8 [Optional] To enable broadcasting of the ESSID, select the **Broadcast ESSID** check box. This makes this wireless network visible to clients scanning for wireless networks. Disabling the ESSID broadcast should not be considered a security measure; clients can still connect if they know the ESSID, and it is possible for network sniffers to read the ESSID from other clients.

9 [Optional] if there is interference from another access point, select another channel the operating frequency or channel for the wireless network from the **Channel/Frequency** list. The channels and frequencies that appear depend on the region selected in the advanced settings. For further information, see “Configuring advanced wireless features” on page 116. Available options (USA, FCC region) are:

- 1/2412 MHz (default)
- 2/2417 MHz
- 3/2422 MHz
- 4/2427 MHz
- 5/2432 MHz
- 6/2437 MHz
- 7/2442 MHz
- 8/2447 MHz
- 9/2452 MHz
- 10/2457 MHz
- 11/2462 MHz

***Tip:** Changing to a different channel may give better performance. Channels do not overlap if they are at least 5 channels apart. For example, channels 1, 6, and 11 do not overlap.*

10 [Recommended only if all wireless clients are trusted] To bridge between clients, select the **Bridge Between Clients** check box. This setting enables the access point to forward packets between clients at the wireless level so that wireless clients are able to “see” each other. This means that packets between wireless clients are not restricted by the firewall. If you disable this setting, but still want to allow access between clients in the firewall, you usually also need to configure each client to route to other clients via the access point.

11 Select a wireless method of security from the **Security Method** list. The fields that appear vary depending on your selection. Available options are:

- **None** — [Not recommended] Select this option for no security and click **Finish**. You have completed your access point configuration.
- **WEP** — Go to step 12 (page 104).
- **WEP with 802.1X** — Go to step 13 (page 105)
- **WPA-PSK** — Go to step 14 (page 106)
- **WPA-Enterprise** — Go to step 15 (page 107).

12 If you chose the **WEP** security method, complete the following fields:

Figure 79: Access Point Configuration — WEP Security Method

The screenshot shows the 'Network Setup' window with tabs for 'Connections', 'Failover & H/A', 'Routes', 'System', and 'DNS'. The 'Direct Connection' sub-tab is active, and the 'Access Point Configuration' section is expanded. The configuration fields are as follows:

Field	Value
MAC Address	00:0E:8E:01:06:CF
ESSID	Test
Broadcast ESSID	<input checked="" type="checkbox"/>
Channel/Frequency	1 / 2412 MHz
Bridge Between Clients	<input type="checkbox"/>
Security Method	WEP
WEP Authentication	Open System (recommended)
WEP Key Length	64 bit (aka 40 bit)
Transmit Key	WEP Key 1
WEP Key 1	
WEP Key 2	
WEP Key 3	
WEP Key 4	

At the bottom of the window are three buttons: 'Back', 'Finish', and 'Cancel'.

- a** Select an authentication from the **WEP Authentication** list. Available options are:
- **Open System** — [Recommended] Allow any client to authenticate. Since clients must still have a valid WEP key in order to send or receive data, this setting does not make the WEP protocol less secure, and is the recommended setting.
 - **Shared Key** — Clients must use the WEP key to authenticate.
 - **Open System or Shared Key** — Allow clients to connect using either of the above two methods.



Security Alert: Due to flaws in the authentication protocol, the Shared Key method reduces the security of the WEP key. Secure Computing recommends using **Open System** authentication instead.

- b** Select a key length from the **WEP Key Length** list. This sets the length of the WEP key fields 1-4. Available options are:
- 128-bit [Recommended] if possible
 - 64-bit

c Select the default **Transmit key**. Available options are:

- WPA Key 1
- WPA Key 2
- WPA Key 3
- WPA Key 4

d Enter up to 4 encryption keys in the **WPA Key 1-4** fields. Accepted formats are:

- 10 hexadecimal digits (0 – 9, A – F) for 64-bit keys
- 26 hexadecimal digits for 128-bit keys.

e Click **Finish**.

13 If you chose **WEP with 802.1X** from the **Security Method** list, click **Finish**.

Figure 80: Access Point Configuration — WEP with 802.1X Security Method

The screenshot shows the 'Network Setup' dialog box with the 'Access Point Configuration' tab selected. The 'Direct Connection' sub-tab is also active. The configuration fields are as follows:

Access Point Configuration	
MAC Address	00:0E:8E:01:06:CF
ESSID	Test
Broadcast ESSID	<input checked="" type="checkbox"/>
Channel/Frequency	1 / 2412 MHz
Bridge Between Clients	<input type="checkbox"/>
Security Method	WEP with 802.1X

At the bottom of the dialog are three buttons: 'Back', 'Finish', and 'Cancel'.

14 If you chose **WPA-PSK** as a security method:

Figure 81: Wireless Configuration — Access Point Configuration page — WPA-PSK

The screenshot shows a web-based configuration interface titled "Network Setup". It has several tabs: "Connections", "Failover & H/A", "Routes", "System", "DNS", and "IPv6". The "Wireless Configuration" tab is selected. Under this tab, there is a sub-section titled "Access Point Configuration". The fields in this section are: "MAC Address" (00:0E:8E:01:06:CF), "ESSID" (Test), "Broadcast ESSID" (checked), "Channel/Frequency" (1 / 2412 MHz), "Bridge Between Clients" (unchecked), "Security Method" (WPA-PSK), "WPA Encryption" (TKIP), and "WPA Key" (abcd1234). At the bottom of the form are "Finish" and "Cancel" buttons.

- a** Select a WPA encryption from the **WPA Encryption** list. Available options are:
- **TKIP (Temporary Key Integrity Protocol):** TKIP is more commonly supported by wireless clients, but is less secure than AES.
 - **AES (Advanced Encryption Standard):** AES is more secure, but might not be supported by legacy wireless clients.

Note: Selecting **AES** for **WPA-PSK** provides **WPA2 802.11i** support, which is also referred to as **WPA2**.

- b** Specify the preshared key in the **WPA Key** field. Allowed formats are:
- 8 to 63 ASCII characters of any type; at least 20 characters at a minimum recommended
 - Exactly 64 hexadecimal characters (0-9, a-b, A-B)
- c** Click **Finish**.

15 If you chose **WPA-Enterprise** as a security method:

Figure 82: Access Point Configuration — WPA-Enterprise Security Method

The screenshot shows the 'Network Setup' window with the 'Direct Connection' tab selected. Inside this tab, the 'Access Point Configuration' sub-tab is active. The configuration fields are as follows:

Field	Value
MAC Address	00:0E:8E:01:06:CF
ESSID	Test
Broadcast ESSID	<input checked="" type="checkbox"/>
Channel/Frequency	1 / 2412 MHz
Bridge Between Clients	<input type="checkbox"/>
Security Method	WPA-Enterprise
WPA Encryption	TKIP

At the bottom of the window are three buttons: 'Back', 'Finish', and 'Cancel'.

- a Select a WPA encryption from the **WPA Encryption** list. Available options are:
 - **TKIP (Temporary Key Integrity Protocol):** TKIP is more commonly supported by wireless clients, but is less secure than AES.
 - **AES (Advanced Encryption Standard):** AES is more secure, but might not be supported by some older wireless clients.
- b Click **Finish**.

Bridging wireless and LAN connections

Use this procedure to configure your wireless connection in access point mode, which automatically bridges your wireless connection to your LAN. The wireless and wired LAN interfaces share a single IP address.

Note: Creating or deleting a bridge between the LAN and the wireless causes a MAC address change for the LAN IP address. Your PC needs to detect this change and perform another ARP (Address Resolution Protocol) lookup before you can contact this IP address again. For Windows, this may take several minutes.

- 1 From the **Network Setup** menu, click **Network Setup**. The **Connections** tab opens.

Figure 83: Wireless Configuration — Access Point option

Network Setup

Connections

Failover & H/A

Routes

System

DNS

IPv6

Name	Port	Current Details	Change Type
Switch A	A	LAN, Static, 192.168.0.1	Direct Connection
Port B	B	Unconfigured	Unconfigured
Wireless	Wireless	Unconfigured	Unconfigured
COM1	COM1	Unconfigured	Unconfigured

Retry unsuccessful connections

Retry

Unconfigured

Access Point

Direct Connection

- 2 Next to the **Wireless** network interface, select **Access Point** from the **Change Type** list. The Access Point page appears.

Figure 84: Wireless Configuration — Access Point page

The screenshot shows the 'Network Setup' window with the 'Wireless Configuration' tab selected. Under the 'Access Point Configuration' section, the following fields are visible:

- MAC Address:** 00:0E:8E:01:06:CF
- ESSID:** Test
- Broadcast ESSID:** ☒
- Channel/Frequency:** 1 / 2412 MHz
- Bridge Between Clients:** ☐
- Security Method:** WPA-PSK
- WPA Encryption:** TKIP
- WPA Key:** abcd1234

At the bottom of the configuration section are 'Finish' and 'Cancel' buttons.

- 3 Complete the fields as desired:
 - a Enter an **ESSID** and select the **Broadcast ESSID** check box.
 - b Select a **Channel/Frequency**. There are 11 channels with frequencies ranging from 2412 to 2462 MHz in 5 MHz increments.
 - c To bridge between trusted wireless clients using a WPA security method, select the **Bridge Between Clients** check box. Packets between bridged wireless clients will not be restricted by the firewall.

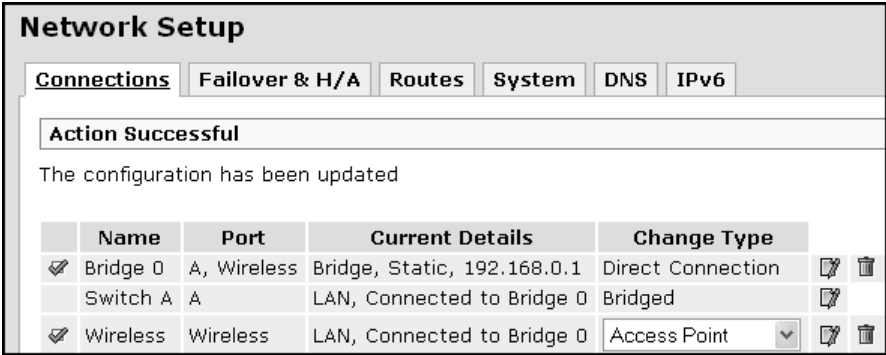
Note: If this setting is disabled, it is still possible to configure wireless clients to access each other via the SnapGear appliance. You need to configure the clients to route to each other by way of the SnapGear appliance. If you have set the firewall class for the wireless interface to Guest, you also need to configure packet filter rules to allow the access.

- d Select a **WPA Security Method** and enter a key.

Make note of these settings for configuring the wireless network connections for wireless clients. For more details about these fields, see the field descriptions in the procedure “Configuring a wireless connection” on page 100.

- 4 Click **Finish**. An action successful message is displayed, and the wireless is bridged to the LAN. Notice in Figure 85 that Switch A and Wireless are now bridged. You can edit or delete the bridge as necessary. If you have a Windows client, be sure to allot extra time for the bridge deletion to complete.

Figure 85: Wireless Configuration — Access Point page



Configuring Wireless MAC-based ACL

Use this procedure to configure an ACL (Access Control List) based on the MAC addresses of the wireless clients. By default, the Wireless ACL is disabled. When the wireless ACL is disabled, any wireless client with the correct ESSID (and encryption key if applicable) can connect to the wireless network. For additional security, you can specify a list of MAC addresses (network hardware addresses) to either allow or deny.



Security Alert: MAC-based ACL is a weak form of authentication, and does not provide any data privacy (encryption). MAC addresses can be forged relatively easily.

- 1 From the **Network Setup** menu, click **Network Setup**. The **Connections** tab opens. On the Connections page, click the **Edit** icon alongside the **Wireless** network interface.
- 2 Click **Wireless Configuration** tab > **ACL** tab.

Figure 86: Wireless ACL-MAC

The screenshot shows the 'Network Setup' window with the 'Wireless Configuration' tab selected. Under 'Wireless Configuration', the 'ACL' sub-tab is active. The 'Access Control List Configuration' section contains three radio buttons: 'Disable Access Control List' (which is selected), 'Allow authentication for MAC addresses in the Access Control List', and 'Deny authentication for MAC addresses in the Access Control List'. Below these are 'Update' and 'Cancel' buttons. The 'Access Control List' section below shows a 'MAC' label and a text box, with the text 'No entries' displayed. An 'Add' button is located at the bottom of this section.

- 3 Select an ACL configuration from the **Mode** options. Available options are:
 - **Disable Access Control List** (Default)
 - **Allow authentication for MAC address in the Access Control List:** Only allows access to the MAC addresses you specify.
 - **Deny authentication for MACs in the Access Control List:** Denies access to all MAC addresses defined in the ACL list.
- 4 Click **Update**.
- 5 Enter a MAC address in the **MAC** field. The address can be an Ethernet MAC address of the form **AA : BB : CC : DD : EE : FF**, where each of the components is a hexadecimal digit.
- 6 Click **Add**. The MAC address appears in the Access Control List.

Figure 87: Wireless ACL-
MAC

The screenshot shows the 'Network Setup' window with the 'Wireless Configuration' tab selected. Under 'Wireless Configuration', the 'ACL' sub-tab is active. A message box states 'Action Successful' and 'The configuration has been updated'. Below this, the 'Access Control List Configuration' section shows 'Mode' with three radio buttons: 'Disable Access Control List', 'Allow authentication for MAC addresses in the Access Control List' (which is selected), and 'Deny authentication for MAC addresses in the Access Control List'. There are 'Update' and 'Cancel' buttons. The 'Access Control List' section contains a table with one entry: 'MAC' with the value '00:11:22:AB:AC:AD' and a delete icon. Below the table is a 'MAC' input field and an 'Add' button.

Network Setup

Connections | Failover & H/A | Routes | System | DNS | IPv6

Direct Connection | **Wireless Configuration** | Aliases | IPv6

Access Point | **ACL** | WDS | Advanced

Action Successful

The configuration has been updated

Access Control List Configuration

Mode

- ☐ Disable Access Control List
- ☒ Allow authentication for MAC addresses in the Access Control List
- ☐ Deny authentication for MAC addresses in the Access Control List

Update **Cancel**

Access Control List

MAC
00:11:22:AB:AC:AD 

MAC

Add

To delete a **MAC** address from the wireless ACL, click its corresponding delete icon.

Configuring WDS

WDS (Wireless Distribution System) allows wireless access points to communicate with each other without the need for a wired Ethernet connection. Since the access point uses a single radio frequency to communicate with both clients and other access points, the available bandwidth is reduced when WDS is enabled.

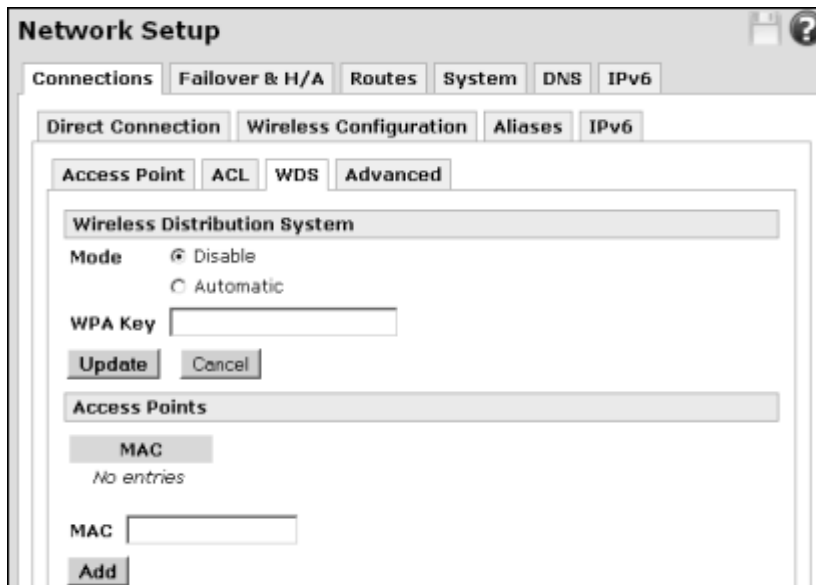
Access points connected using WDS must be configured with the same channel and encryption settings. The ESSID may be the same or different. If the access points have the same ESSID, then clients can transparently roam between them.

There are two common scenarios for WDS: bridging or repeating. *WDS bridging* is when an access point does not allow wireless clients to connect, and simply forwards packets between access points. WDS bridging is used to connect two wired Ethernet connections via a wireless link. *WDS repeating* is when an access point allows wireless clients to connect, and forwards packets from these clients to another access point. This is used to extend the wireless coverage without requiring the additional access points to be connected to a wired Ethernet connection.

Tip: *Wireless client performance will decrease when activating WDS due to the single radio frequency used to communicate with both clients and other access points. To ensure the maximum available bandwidth for wireless clients, consider using wired Ethernet connections if possible instead of WDS repeating to link wireless access points.*

- 1 From the **Network Setup** menu, click **Network Setup**. The **Connections** tab opens. On the Connections page, click the **Edit** icon alongside the **Wireless** network interface.
- 2 Click **Wireless Configuration** tab > **WDS** tab.

Figure 88: WDS



- 3 In the **Wireless Distribution System** pane, select an option for **Mode**. This is the mode that WDS is operating in. Available options are:
 - **Disable** — Disables WDS completely.
 - **Automatic** — Enables bridging or repeating as appropriate. If the wireless interface is unconfigured, then bridging is enabled (wireless clients cannot connect). Otherwise repeating is enabled.
- 4 Specify the WPA preshared key that is used for the WDS link in the **WPA Key** field. This key is only used if the Access Point security method is configured for **WPA-PSK** or **WPA-Enterprise**. If the Security Method is set to **WEP**, then the same WEP Key is used for both the wireless clients and the WDS link.

Note: You cannot enable both WDS and WEP with 802.1X.

- Can be exactly 64 hexadecimal characters (0-9, a-b, or A-B)
 - Can be from 8 to 63 characters of any type
- 5 Click **Update**.
 - 6 In the **Access Points** pane, specify the MAC address of an Access Point to create a WDS link to, and then click **Add**. You can create up to 8 WDS links.

You can delete a WDS link using the delete icon in the WDS page. You can change the MAC address for a WDS link using the edit icon in the **Connections** tab. The MAC address can be Ethernet MAC address of the form AA:BB:CC:DD:EE:FF, where each component is a hexadecimal digit.

Configuring WDS bridging

Use this procedure to configure WDS bridging.

- 1 Configure the wireless settings on the **Access Point** tab.
- 2 Select the **WDS** tab.
- 3 Set **Mode** to **Automatic**.
- 4 Click **Add** and enter the **MAC** of the peer Access Point.
- 5 Click the **Connections** tab.
- 6 Create a new **Bridge**. Select both the LAN interface and the WDS interface to be on the bridge.
- 7 Leave the **Wireless** port unconfigured.
- 8 Configure the peer Access Point in a similar manner.

Configuring WDS repeating

Use this procedure to configure WDS repeating.

- 1 Configure the wireless settings on the **Access Point** tab.
- 2 Select the **WDS** tab.
- 3 Set **Mode** to **Automatic**.
- 4 Click **Add** and enter the **MAC** of the main Access Point.
- 5 Click the **Connections** tab.
- 6 Create a new **Bridge**. Select both the Wireless interface and the WDS interface to be on the bridge.
- 7 Configure the main Access Point in a similar manner; however, it will typically include the LAN interface on the bridge.

Configuring automatic WDS bridging and repeating

Use this procedure to configure WDS bridging and repeating:.

- 1 Configure the wireless settings on the **Access Point** tab.
- 2 Select the **WDS** tab.
- 3 Set **Mode** to **Automatic**.
- 4 Click **Add** and enter the **MAC** of the main Access Point.
- 5 Click the **Connections** tab, create a new **Bridge**. Select the Wireless interface, the LAN interface, and the WDS interface to all be on the bridge.

Configuring advanced wireless features

Use this procedure to configure advanced wireless settings. The default settings should be sufficient for most configurations. Make sure the correct region is configured for your access point, since the region setting restricts channels and frequencies in accordance with the local regulatory organization. Tweaking these advanced wireless features can increase processing overhead, so balance performance requirements with this in mind. Advanced wireless settings include packet fragmentation, RTS (Request to Send), and beacon frames.

Normally, when a packet has an error, the entire packet must be retransmitted. If packet fragmentation is enabled, the packet is split up into smaller fragments, and thus only the fragment that has an error needs to be retransmitted, which increases performance. Fragmentation incurs an overhead per fragment, so enabling it when it is not needed decreases performance.

RTS is used to negotiate when wireless clients can transmit. If you have two wireless clients out of range of each other but both still within range of the access point, they may both attempt to transmit at the same time, which causes a collision. Enabling RTS avoids these collisions, and thus increases performance. RTS incurs an overhead for transmitting, so enabling it when it is not needed decreases performance. Since the access point is in range of all wireless clients, you would not typically enable RTS for an access point.

Beacon frames are used to coordinate the wireless network. Sending beacon frames more often (that is, using a lower beacon interval) increases responsiveness, but decreases performance due to higher overheads. A DTIM (Delivery Traffic Indication Message) is periodically included in the beacon frame. A DTIM indicates to clients in power-saving mode that there are packets for them to receive. Sending a DTIM more frequently increases responsiveness for clients in power-saving mode, but uses more electrical power since the clients must stay awake longer.

- 1 From the **Network Setup** menu, click **Network Setup > Connections** tab. The Connections tab opens. On the **Connections** tab, click the edit icon alongside the **Wireless** interface.

- 2 Click **Wireless Configuration** tab > **Advanced** tab. The Advanced Configuration page for wireless appears.

Figure 89: Wireless Advanced configuration

The screenshot shows the 'Network Setup' window with the 'Wireless Configuration' tab selected. Within this tab, the 'Advanced' sub-tab is active. The 'Advanced Configuration' section contains the following settings:

- Region:** USA (FCC) (dropdown menu)
- Protocol:** 802.11b and 802.11g (dropdown menu)
- Transmit Power (%):** 100 (text input)
- Preamble Type:** Long (dropdown menu)
- Enable RTS:** ☒ (checkbox)
- RTS Threshold:** 2346 (text input)
- Enable Fragmentation:** ☒ (checkbox)
- Fragmentation Length:** 2345 (text input)
- Beacon Interval (ms):** 100 (text input)
- DTIM Interval (beacons):** 1 (text input)

At the bottom of the configuration area are 'Update' and 'Cancel' buttons.

- 3 Select the region in which the access point is operating from the **Region** list. The region setting restricts the allowable frequencies and channels. If your region is not listed, select a region that has similar regulations.
- 4 Select a protocol from the **Protocol** list. Available options are:
 - **802.11b only:** Wireless clients can only connect using 802.11b (11 Mbit/s). Most wireless clients that support 802.11g also support 802.11b.
 - **802.11g only:** Wireless clients can only connect using 802.11g (54 Mbit/s). Wireless clients that only support 802.11b are unable to connect.
 - **802.11b and 802.11g:** [Recommended, default] Both 802.11b and 802.11g wireless clients can connect.

Note: Be aware that all clients need to connect using the same protocol. As such, if 802.11b clients connect, all wireless connections will be using the 802.11b protocol, even those clients that support 802.11g.

- 5 Enter the transmit power for the access point in the **Transmit Power (%)** field. Decreasing the power reduces the range of the wireless network and reduces interference to other nearby access points. The field attributes are as follows:
 - Range: 1-100
 - Default: 100%
- 6 Select a preamble length from the **Preamble Type** list. The preamble is part of the physical wireless protocol. Available options are:
 - **Long** (Default)
 - **Short**. Short preambles can increase throughput; however, some wireless clients might not support short preambles.
- 7 [Optional] To enable RTS, select the **Enable RTS** check box. Default: Disabled.
- 8 [Conditional; complete if RTS is enabled] Enter a minimum packet size in the **RTS Threshold** field. Collisions are less likely for smaller packets, and so the overhead of using RTS for these might not be worthwhile. The field attributes are as follows:
 - Range 1-2346
 - Default: 2346
- 9 [Optional] To enable, select the **Enable Fragmentation** check box. Default: Disabled.
- 10 Enter a fragment size in the **Fragmentation Length** field. Smaller fragments decrease the amount retransmitted when there is an error; however, it increases the total processing overhead for each packet.
 - Range 256-2345
 - Default: 2345
- 11 Specify the interval between beacon frames in the **Beacon Interval (ms)** field.
 - Range 20-999
 - Default: 100
- 12 Specify how often a DTIM interval is included in the beacon frame in the **DTIM Interval (beacons)** field.
 - Range 1-255
 - Default: 1
- 13 Click **Update**.

Bridging

The appliance can be configured to bridge between network interfaces. When two or more network interfaces are bridged, the appliance learns and keeps track of which hosts reside on either side of the bridge, and automatically directs network traffic appropriately.

One advantage of bridging network interfaces is that hosts on either side of the bridge can communicate with hosts on the other side without having to specify a route to the other network via the appliance. Another advantage is that network traffic not usually routed by an unbridged interface, such as broadcast packets, multicast packets, and any non-IPv4 protocols such as IPv6, IPX, or Appletalk pass over the bridge to their destination host.



Caution: *You must trust all devices that are directly connected to bridged interfaces. Since the firewall does not know which IP addresses for the bridged network belong on which interface, this means it is easy for a directly connected device to spoof an IP address. You can manually add Packet Filter rules to prevent spoofing.*

Furthermore, non-IP protocols are not restricted by the firewall. You should not bridge between interfaces with different firewall classes if you are using non-IP protocols. Bridging only supports Ethernet and GRE network interfaces. Since bridging can only be configured as a Direct Connection, you cannot bridge a PPPoE connection. If you want to bridge a wireless interface to a LAN connection, see “Bridging wireless and LAN connections” on page 108.

Adding a bridged interface

Use this procedure to add a bridged network interface. When network interfaces are bridged, they all share a common configuration for the network connection. This means that a single IP address is used on all of the network interfaces. Bridging network interfaces involves creating and then associating existing network interfaces with a Bridge interface. Once this bridge interface has been added, it appears on the Network Setup page under the Connections tab, along with the SnapGear appliance’s other network interfaces.

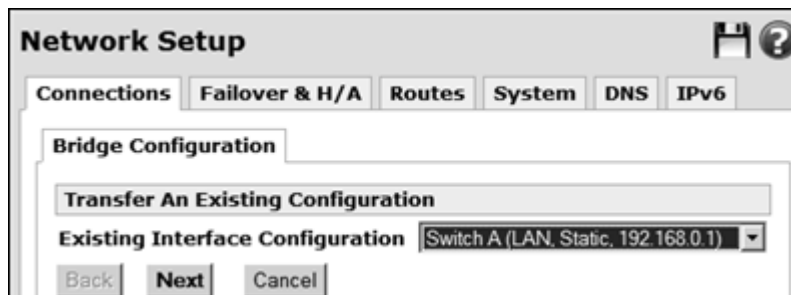
Prerequisites:

- If high availability is configured for a connection, it must be modified or disabled before bridging.
- A bridge cannot include multiple VLANs on the same switch.
- If a DHCP server is used for a connection, and the bridge you are adding uses a static IP, then the settings are incompatible. DHCP must be disabled or deleted.

To add a bridge

- 1 From the **Network Setup** menu, click **Network Setup > Connections** tab.
- 2 From below the main Connections table, select **Bridge** from the list and click **Add**. The Bridge Configuration tab appears.

Figure 90: Network Setup
Edit Bridge Configuration
page



- 3 If you want to transfer the IP address settings of an existing network connection to the bridge interface, select it from the **Existing Interface Configuration** list. Otherwise, click **None**.

Note: Since the appliance automatically directs network traffic, hosts on either side do not need to specify this IP address as a gateway to the networks connected to the bridge. It is not so important which IP address you choose to assign to the bridge interface; it is primarily used by hosts on either side of the bridge only to connect to the management console of the appliance. Specific routes are still required to reach networks that are not being bridged.

- 4 Click **Next**. If you selected an existing interface, the Edit Bridge Configuration page appears. Skip to step 5. If you selected **None**, the Direct Connection Settings page appears.

Figure 91: Direct
Connection Settings page
(bridging)

The screenshot shows a window titled "Network Setup" with a tabbed interface. The "Connections" tab is selected. Inside this tab, the "Bridge Configuration" sub-tab is active. Under "Bridge Configuration", there is a section titled "Direct Connection Settings". This section contains the following fields and controls:

- Connection Name:** A text input field.
- DHCP assigned:** A checkbox.
- IP Address:** A text input field.
- Subnet Mask:** A text input field containing the value "24".
- Gateway:** A text input field.
- DNS Server(s):** A text input field.
- Firewall Class:** A dropdown menu with "Bridge" selected.

At the bottom of the "Direct Connection Settings" section are three buttons: "Back", "Next", and "Cancel".

- a [Optional] Enter a connection name.
 - b Either indicate the DHCP is assigned by selecting the **DHCP assigned** check box, or enter an **IP address**.
 - c [Conditional if not using DHCP] Enter the **Subnet Mask**.
 - d [Optional, can be left blank] Enter the IP address for the **Gateway**.
 - e [Optional, can be left blank] Enter the IP address for the **DNS Server**.
 - f Click **Next**. The Edit Bridge Configuration page appears. Continue with the next step.
- 5 The Edit Bridge Configuration tab appears.

Figure 92: Network Setup
Edit Bridge Configuration
page

Network Setup

ConnectionsFailover & H/ARoutesSystemDNSIPv6

Bridge Configuration

Edit Bridge Configuration

Interface	Bridged	Firewall Class
Switch A (Static)	<input checked="" type="checkbox"/>	LAN
Port A4 (Port A4, DHCP)	<input type="checkbox"/>	Internet
Port B (Static)	<input type="checkbox"/>	Internet
WIFI (Wireless, Static)	<input type="checkbox"/>	LAN
GRE Tunnel 1	<input type="checkbox"/>	Guest

Enable Spanning Tree Protocol

☐

Forwarding Delay

0

Back

Finish

Cancel

- 6 For each network interface you want to bridge, select the **Bridged** check box. Selecting this check box for an interface places the interface on the bridge.



Important: If a network interface is placed on the bridge, its current configuration is deleted.

- 7 Ensure its **Firewall Class** is set appropriately.
- 8 [Optional] If you have multiple bridges connected together on your network, select the **Enable Spanning Tree Protocol** check box. This setting allows the bridges to exchange information, helping to eliminate loops and find the optimal path for network traffic.

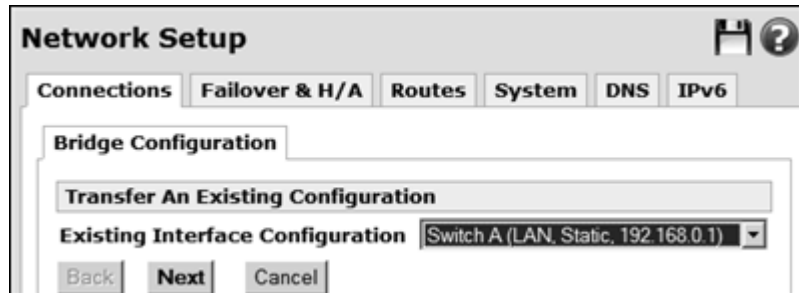
- 9 Enter the time in seconds between when the bridge interface comes online and when it begins forwarding packets in the **Forwarding Delay** field. The delay usually only occurs when the appliance first boots, or when the bridge configuration is modified. This delay allows the appliance's bridge to detect which hosts are connected to each of the bridge's interfaces, rather than blindly sending network traffic out all network interfaces.
 - Can be zero (0) or greater
- 10 Click **Next** to review or change IP address information for the bridge interface, otherwise click **Finish**.

**Example 1:
Transferring
existing settings
while adding a new
bridge**

This example steps through the sequence when transferring the IP address settings of an existing network connection to the bridge interface you are adding.

- 1 From the **Network Setup** menu, click **Network Setup > Connections** tab. The Connections page appears.
- 2 From below the main Connections table, select **Bridge** from the list and click **Add**. The Bridge Configuration tab appears.
- 3 Select the interface from the **Existing Interface Configuration** list. This example transfers the settings from the Switch A LAN interface.

Figure 93: Example transfer configuration to bridge



- 4 Click **Next**. The Edit Bridge Configuration tab appears.

Figure 94: Network Setup
Edit Bridge Configuration
page

5 Select the check box for the other Interface you want to bridge.

Interface	Bridged	Firewall Class
Switch A (Static)	<input checked="" type="checkbox"/>	LAN
Port A4 (Port A4, DHCP)	<input type="checkbox"/>	Internet
Port B (Static)	<input type="checkbox"/>	Internet
WIFI (Wireless, Static)	<input type="checkbox"/>	LAN
GRE Tunnel 1	<input type="checkbox"/>	Guest

Enable Spanning Tree Protocol ☐

Forwarding Delay

Back Finish Cancel

6 Click **Finish**.

Example 2: Adding a bridge sans transfer

This example steps through the sequence when simply adding a new bridge interface without transferring settings from an existing configuration.

- 1 From the **Network Setup** menu, click **Network Setup > Connections** tab. The Connections page appears.
- 2 From below the main Connections table, select **Bridge** from the list and click **Add**. The Bridge Configuration tab appears.
- 3 From the **Existing Interface Configuration** list, select **None**.
- 4 Click **Next**. The Bridge Configuration tab containing the Direct Connection Settings page opens.

Figure 95: Bridge Configuration Direct Connection Settings page

- 5 Enter **test_bridge** in the **Connection Name** field.
- 6 Enter **1.1.1.3** in the **IP Address** field.
- 7 Click **Next**. The Edit Bridge Configuration page appears. Notice that there are not any selections in the **Bridged** column.

Figure 96: Bridge Configuration Direct Edit Bridge Configuration page

Interface	Bridged	Firewall Class
Switch A (Static)	<input type="checkbox"/>	
Port A4 (Port A4, DHCP)	<input type="checkbox"/>	Internet
Port B (Static)	<input type="checkbox"/>	Internet
WIFI (Wireless, Static)	<input type="checkbox"/>	LAN
GRE Tunnel 1	<input type="checkbox"/>	Guest

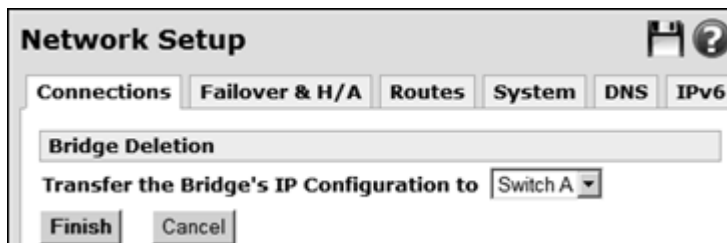
- 8 Select the **Bridged** check boxes for Switch A and Port B.
- 9 Click **Finish**.

Deleting a bridge

Use this procedure to delete a bridge. Deleting a bridge transfers the IP configuration of the bridge to another interface.

- 1 From the Network Setup menu, click **Network Setup > Connections** tab. The Connections page opens.
- 2 Click the delete icon for the bridge you want to delete. The Bridge Deletion page appears.

Figure 97: Bridge Deletion page



- 3 Select the interface to which to transfer the bridge's IP configuration, if available, or select **None**.
- 4 Click **Finish**.

Bridging across a VPN connection

Bridging across a VPN connection is useful for:

- Sending IPX/SPX over a VPN, something that is not supported by other VPN vendors.
- Serving DHCP addresses to remote sites to ensure that they are under better control (which can also be achieved with a DHCP relay. See "DHCP Relay page" on page 171).
- Allowing users to make use of protocols that do not work well in a WAN environment (such as *netbios*).

VLAN

Note: VLANs are not supported by the SG300.

VLAN (Virtual Local Area Network) is a method of creating multiple virtual network interfaces using a single physical network interface. Packets in a VLAN are simply Ethernet packets that have an extra four bytes immediately after the Ethernet header. The format for these bytes is defined by the standard IEEE 802.1Q. Essentially, they provide for a VLAN ID and a priority. The VLAN ID is used to distinguish each VLAN. A packet containing a VLAN header is called a *tagged* packet.

When a packet is routed out the VLAN interface, the VLAN header is inserted and then the packet is sent out on the underlying physical interface. When a packet is received on the physical interface, it is checked for a VLAN header. If present, the router makes it appear as though the packet arrived on the corresponding VLAN interface.



Caution: Since the addition and removal of the VLAN header are performed in software, any network device can support VLANs. Further, this means that VLANs should not be used for security unless you trust all the devices on the network segment.

Once added, VLAN interfaces can be configured as if they were additional physical network interfaces. A typical use of VLANs with the SnapGear appliance is to enforce access policies between ports on an external switch that supports port-based VLANs. In this scenario, only the switch and other trusted devices should be directly connected to the LAN port of the SnapGear appliance. The SnapGear appliance and the switch are configured with a VLAN for each port or group of ports on the switch. The switch is configured to map packets between its ports and the VLANs. The SnapGear appliance can then be configured with firewall rules for the VLANs, and these rules are effectively applied to the corresponding ports on the switch.

Additionally, Switch A on the SG560, SG565, and SG580 supports port-based VLANs. One benefit of this feature is that you can assign individual functions to each of the ports on the switch; for example, you might decide to use port A2 to connect to a DMZ, and port A3 as a second Internet connection. For details, see “Port-Based VLANs” on page 129.

Adding a VLAN

- 1 From the **Network Setup** menu, click **Network Setup**. The Connections page appears.
- 2 Select **VLAN** from the list and click **Add**. The VLAN Configuration tab appears.

Figure 98: Network Setup
VLAN Configuration

Port	Mode		
A2	<input type="radio"/> Disabled	<input type="radio"/> Tagged	<input type="radio"/> Untagged
A3	<input type="radio"/> Disabled	<input type="radio"/> Tagged	<input type="radio"/> Untagged
A4	<input type="radio"/> Disabled		

- 3 From the **Interface** list, select the network interface on which to add the VLAN.
- 4 Enter a value for the VLAN ID in the **VLAN ID** field. The value can be a decimal number between 1 and 4094. If this VLAN interface is to participate on an existing VLAN, the VLAN ID number entered in this field must match the ID of the existing VLAN. This ID must be unique amongst the VLANs on this Ethernet interface.
- 5 **Port / Mode:** If this table is displayed, this interface has been enabled for port-based VLANs. For more information, see “Port-Based VLANs” on page 129. Select the VLAN mode for the port. This option is only available when port-based VLANs are enabled. The choices are:
 - **Disabled** — Packets on this VLAN are not sent or received on this port. If a port is disabled for all VLANs, then the port is set to untagged mode for the default VLAN of the switch.
 - **Tagged** — Packets on this VLAN are sent and received on this port as tagged packets that contain a VLAN header. This is identical to how the switch would handle the packet when port-based VLANs are disabled. Devices connected to this port must support VLANs.
 - **Untagged** — Packets on this VLAN are sent and received on this port as untagged packets without a VLAN header. This means that the VLAN ID will only be used while routing the packet within this appliance. Devices connected to this port will not see the VLAN ID on the packet, and do not need to support VLANs. If a port is set to untagged, then that port must be set to disabled for all other VLANs. A port can be set to tagged for multiple VLANs. It is also allowable for more than one port to be set to untagged for a given VLAN.

- 6 Click **Update**. You have now added a tagged VLAN interface that you can configure as you would any other network interface. Select the connection type from the **Change Type** list and configure a connection for the VLAN interface.

Port-Based VLANs

Note: *Port-based VLAN is applicable to models SG560, SG565, and SG580 only.*

A port-based VLAN configuration is required for certain SnapGear models to be configured for an additional WAN, LAN, or DMZ. The SG560, SG565, and SG580 models have a built in VLAN-capable switch. This gives you the flexibility to either use it as a simple switch that allows access between all ports (the default), or use port-based VLANs to control access between each individual port in the switch. This port-based VLAN configuration makes it possible to: assign each of the four ports its own subnet address; declare it to be a LAN, WAN, or DMZ independent of the other ports; or treat the switch port as if it were a completely separate physical port.

The SnapGear appliance can also participate on an existing VLAN. When you add a VLAN interface to connect to the existing VLAN, you can associate the VLAN with one or more SnapGear ports.

Tagged and untagged VLANs

When using port-based VLANs, it is important to understand the differences between tagged and untagged VLANs. Tagged VLAN interfaces add a VLAN header (see "VLAN" on page 127) to outgoing network packets, and only accept incoming network packets that contain an appropriate VLAN header. Untagged VLAN interfaces do not add a VLAN header to outgoing network packets, and do not accept incoming packets containing a VLAN header.

A port can be a member of either a single untagged VLAN, or one or more tagged VLANs. A port cannot be a member of both tagged and untagged VLANs.

Once Switch A has port-based VLANs enabled, ports that have not been explicitly assigned to one or more VLANs are assigned to the default VLAN, which is untagged.

Typically, a tagged VLAN interface is used when you want to join an existing VLAN on the network, and an untagged VLAN interface is used when you are using the port-based VLAN feature to isolate the ports so that you can configure each of them individually.

Rules and limitations of port-based VLANs

There are few rules and limitations to keep in mind when using port-based VLANs:

- **Switch A** can only have one default VLAN, and any ports that are not explicitly assigned to another VLAN are automatically placed on the default VLAN. The default VLAN is untagged.
- You cannot add tagged VLANs to port **A1**; it is a member of the default VLAN only.
- The total bandwidth from the switch into the CPU is 100 Mbits/s, which is shared between the four ports. This may limit the bandwidth available to a single port when perform general routing, packet filtering, and other activities.
- Port-based VLANs can only be enabled if there are less than 16 total VLANs.

Enabling port-based VLANs

Use this procedure to enable a port-based VLAN, which isolates each port in the switch. This allows you to connect different networks to each port, and to enforce firewall policies between ports.

***Tip:** If you previously selected 1 LAN Port, 3 Isolated Ports in the Switch Configuration step of the Quick Setup Wizard, port-based VLANs are already enabled and a single isolated VLAN for each port has already been added. You can also run the wizard again to select this feature, skipping the options that are already configured. To relaunch the wizard, click the Secure Computing logo in the upper left above the menu, or open the console in a fresh browser window.*

- 1 From the **Network Setup** menu, click **Network Setup**. The Connections page appears.
- 2 Next to the port-based VLAN-capable interface (**Switch A** on the SG560, SG565 and SG580), click the edit icon.

Figure 99: Connections page—Switch A interface

Connections					Failover & H/A	Routes	System	DNS	IPv6
Name		Port	Current Details			Change Type			
Switch A		A1	LAN, Static, 192.168.0.1			Direct Connection			

- 3 Click the **Ethernet Configuration** tab. The Ethernet Configuration page appears.

Figure 100: Ethernet Configuration—Configure Ethernet Port page

Network Setup

Connections | Failover & H/A | Routes | System | DNS | IPv6

Direct Connection | **Ethernet Configuration** | Aliases | IPv6

Configure Ethernet Port

Port: A1, A2, A3, A4
 Name: Switch A
 Current Details: LAN, Static, 192.168.0.1
 MAC Address: 00:D0:CF:04:F0:32
 MTU: 1500

Port	Ethernet Speed
A1	Default Auto Negotiation
A2	Default Auto Negotiation
A3	Default Auto Negotiation
A4	Default Auto Negotiation

Enable Port-based VLANs: ☒
 Default Port-based VLAN ID: 2

Update Cancel

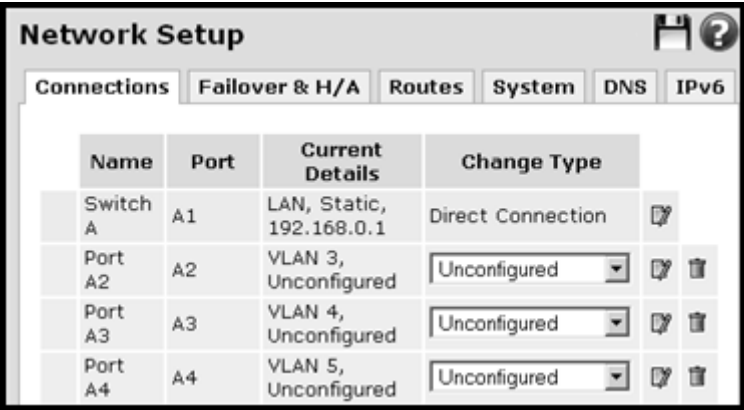
- 4 Select the **Enable port-based VLANs** check box.
- 5 As the default VLAN is always untagged, typically you only need to change the **Default port-based VLAN ID** from the default setting of 2 if you want another port to participate on an existing tagged VLAN with the ID of 2.
 - Default: 2
 - Range: 1-4094
- 6 Click **Update**.

Adding a port-based VLAN

Use this procedure to manually add a port-based VLAN on the switch of a SnapGear appliance.

Tip: If you previously selected the **1 LAN Port, 3 Isolated Ports** option in the **Switch Configuration** step of the **Quick Setup Wizard**, a single isolated VLAN for each port on the switch has already been added as shown in Figure 101. You can also run the wizard again to select this feature, skipping the options that are already configured. To relaunch the wizard, click the **Secure Computing** logo in the upper left above the menu, or open the console in a fresh browser window. All that remains to do with the wizard approach is configuring the **Mode** and **connection** (**Change Type**) for each port.

Figure 101: Isolated ports



The screenshot shows the 'Network Setup' window with the 'Connections' tab selected. It displays a table with columns: Name, Port, Current Details, and Change Type. The table lists four items: 'Switch A' (LAN, Static, 192.168.0.1), 'Port A2' (VLAN 3, Unconfigured), 'Port A3' (VLAN 4, Unconfigured), and 'Port A4' (VLAN 5, Unconfigured). Each port row has a dropdown menu set to 'Unconfigured' and icons for editing and deleting.

Name	Port	Current Details	Change Type
Switch A	A1	LAN, Static, 192.168.0.1	Direct Connection
Port A2	A2	VLAN 3, Unconfigured	Unconfigured
Port A3	A3	VLAN 4, Unconfigured	Unconfigured
Port A4	A4	VLAN 5, Unconfigured	Unconfigured

- 1 From the **Network Setup** menu, click **Network Setup**. The **Connections** page appears.
- 2 Select **VLAN** from the list and click **Add**.

Figure 102: Select VLAN from virtual interface list

Network Setup

Connections Failover

Name	Port
Switch A	A1
<input checked="" type="checkbox"/> testVLAN	A2, A3, A4
<input checked="" type="checkbox"/> Port B	B
<input checked="" type="checkbox"/> WIFI	Wireless
<input checked="" type="checkbox"/> COM1	COM1

Retry unsuccessful connections

Add Bridge

Bridge
GRE Tunnel
VLAN

The Edit VLAN Configuration page appears.

Figure 103: Edit port-based VLAN configuration

Network Setup

Connections Failover & H/A Routes Sys

VLAN Configuration

Edit VLAN Configuration

Interface Switch A

VLAN ID

Port	Mode		
A2	<input type="radio"/> Disabled	<input type="radio"/> Tagged	<input type="radio"/> Untagged
A3	<input type="radio"/> Disabled	<input type="radio"/> Tagged	<input type="radio"/> Untagged
A4	<input type="radio"/> Disabled	<input type="radio"/> Tagged	<input type="radio"/> Untagged

Update Cancel

- From the **Interface** list, select the port-based VLAN-capable interface on which to add the VLAN (**Switch A**).

- 4 If you are adding a VLAN interface to participate on an existing VLAN, enter its ID number in the **VLAN ID** field. Otherwise, if there is not an existing VLAN, enter the next available VLAN ID. If the **Default port-based VLAN ID** on the Ethernet Configuration page (see Figure 100 on page 131) has been left at its default setting of 2, **Port A2** uses VLAN ID 3, **Port A3** uses VLAN ID 4, and so forth.

***Note:** Some Cisco equipment uses tagged VLAN 1 for its own purposes. Secure Computing recommends setting the default VLAN ID to 2 or greater for tagged VLANs, unless you intend for the SnapGear appliance and Cisco equipment to interact over tagged VLAN 1.*

- 5 In the **Mode** table, associate the Switch A ports (**A2, A3, A4**) with this VLAN interface:
 - To exclude a port or ports from the VLAN, click **Disabled**.
 - If you are configuring a port or ports to participate on an existing tagged VLAN, click **Tagged**.
 - To isolate a single port for individual configuration, click **Untagged**. Packets on this VLAN are sent and received on this port as untagged packets, which means that the VLAN ID will only be used while routing the packet within this unit. Devices connected to this port will not see the VLAN ID on the packet, and do not need to support VLANs. If a port is set to untagged, then that port must be set to disabled for all other VLANs. It is allowable for a port to be set to tagged for multiple VLANs. It is also allowable for more than one port to be set to untagged for a given VLAN. For information on tagged versus untagged VLAN, see “Tagged and untagged VLANs” on page 129.
- 6 Click **Update**. This VLAN interface now appears as **Unconfigured** in the Connections page. You can configure the VLAN interface as you would any other network interface.

Editing a VLAN

Use this procedure to edit a port-based or standard VLAN configuration.

- 1 From the **Network Setup** menu, click **Network Setup**. The Connections page appears.
- 2 Click the edit icon for the VLAN you want to edit. The edit page for the connection appears.
- 3 Click the **VLAN Configuration** tab. The Edit VLAN Configuration page appears.
- 4 Make your changes and click **Update**.

Deleting a VLAN

Use this procedure to delete a port-based or standard VLAN configuration.

- 1 From the **Network Setup** menu, click **Network Setup**. The Connections page appears.
- 2 Click the delete icon for the VLAN. You are prompted to confirm the delete. Click **OK**.

GRE tunnels

The GRE (Generic Routing Encapsulating) configuration of the SnapGear appliance allows you to build GRE tunnels to other devices that support the GRE protocol. You can build GRE tunnels to other SnapGear appliances that support GRE, or to other devices such as Cisco equipment. A GRE tunnel must be created between a local IP address and a remote IP address that can already route between each other. Typically, these addresses are LAN IP addresses accessible via a VPN tunnel. It is useful to create alias addresses on LAN interfaces for this purpose, so that the LAN IP addresses can be routed over the GRE tunnel as well.



Security Alert: GRE tunnels are not secure unless they are run over another secure protocol. When using a GRE tunnel that runs over the Internet, it is possible for an attacker to put packets onto your network. If you want a tunneling mechanism to securely connect to networks, then you should use IPSec, or tunnel GRE over either IPSec or PPTP tunnels.

Packets can be sent over a GRE tunnel using either static routes or bridging. Using static routes for a GRE tunnel over IPSec avoids having to create the many security associations that would otherwise be needed to deal with multiple subnets at either end. A bridged GRE tunnel is useful for transmitting packets across a VPN connection that would normally be dropped by IP routing. This includes broadcast packets, multicast packets and any non-IP protocol such as IP v6, IPX, or Apple Talk.

The basic steps to set up GRE over IPSec are:

- 1 Create an IPSec tunnel for which the Local Network is the local LAN IP address, and the Remote network is the remote LAN IP address. The prefix length for each network should be /32.
- 2 Create a GRE tunnel for which the Local Address is the local LAN IP address, and the Remote Address is the remote LAN IP address.
- 3 Create static routes that use the GRE tunnel as their interface. See “Routes” on page 139. Do not specify a gateway address.

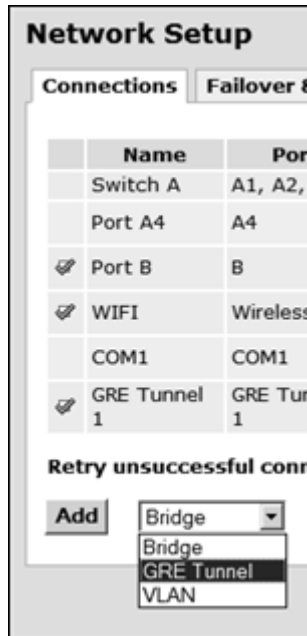
To bridge the local and remote LAN over IPSec:

- 1 Create an alias on the local LAN interface, and another alias on the remote LAN interface.
- 2 Create an IPSec tunnel for which the Local Network is the local alias address, and the Remote Network is the remote alias address. The prefix length should be /32 for each network.
- 3 Create a GRE tunnel for which the Local Address is the local alias address, and the Remote Address is the remote alias address.
- 4 Create a bridge between the LAN interface and the GRE tunnel at each end.

Adding a GRE interface

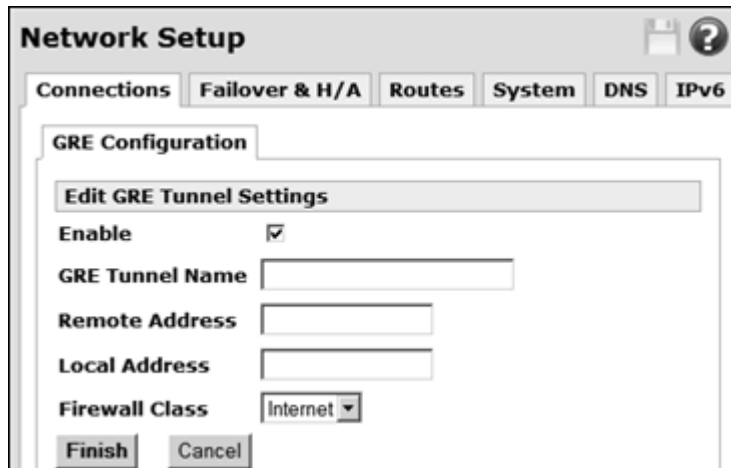
- 1 Click **Network Setup** > **Connections** tab. The Connections page appears.

Figure 104: GRE Tunnel setup



- 2 Select **GRE Tunnel** from the list and click **Add**. The Edit GRE Tunnel Settings page appears.

Figure 105: Edit GRE Tunnel Settings page



- 3 Ensure the **Enable** check box is selected.
- 4 [Optional] Enter a descriptive **GRE Tunnel Name** for this tunnel.

- 5 Enter the address of the remote GRE endpoint in **Remote Address**; for example, the Internet IP address of a remote SnapGear appliance. The IP address can be in the form *a.b.c.d*.
- 6 Enter the address of the local GRE endpoint in the **Local Address** field. This is typically a free address on your main LAN. If your LAN connection has an alias address, it may also be a free address on the alias network. The IP address can be in the form *a.b.c.d*.
- 7 Select a firewall class for the GRE interface from the **Firewall Class** list. Available options are:
 - LAN
 - Internet
 - DMZ
 - Guest
- 8 Click **Finish**. The GRE tunnel now appears in the Connections page.

Troubleshooting GRE tunnels

Symptom: Cannot ping a host on the other side of the GRE tunnel.

- Ensure that there is a route set up on the GRE tunnel to the remote network.
- Ensure that there is a route on the remote GRE endpoint to the network at this end of the GRE tunnel.
- Check that there is a GRE interface created on the appliance. To do this, go to the Diagnostics page (**System menu > Diagnostics > System** tab) and scroll to the bottom. In the **Interface Configuration** section, there should be an interface called **greX**. **greX** is the same as the **Interface Name** specified in the table of current GRE tunnels.
- Also ensure that the required routes have been set up on the GRE interface. This might not occur if you have the same route specified on different GRE tunnels, or on different network interfaces.
- Perform a ping test to ensure that the remote GRE endpoint is reachable. See “Ping test” on page 503.

Symptom: Cannot ping the remote GRE end point.

- Ensure that the remote GRE end point responds to pings.
- Note that by default, no packets are routed across the GRE tunnel unless there is a route set up on the GRE tunnel.

Routes

You can configure static and policy routes for the appliance.

Advanced users can enable route management for RIP, BGP, and OSPF protocols. For more information, see:

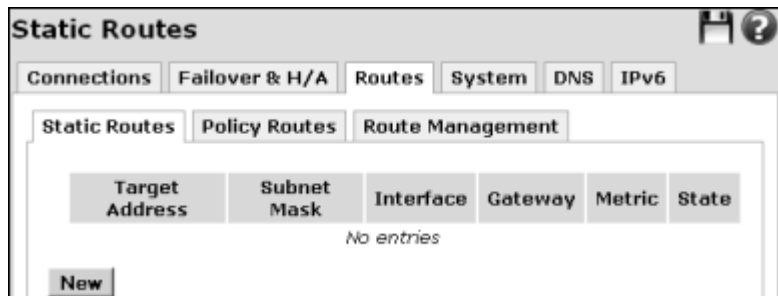
- “Example: Configuring RIP Route Management” on page 144
- “Example: OSPF” on page 146
- “Example: BGP” on page 149

Creating a static route

Use this procedure to add static routes for the SnapGear appliance. These routes are additional to those created automatically by the configuration scripts of the appliance.

- 1 From the **Network Setup** menu, click **Network Setup > Routes tab > Static Routes** tab. The Static Routes page appears.

Figure 106: Static Routes



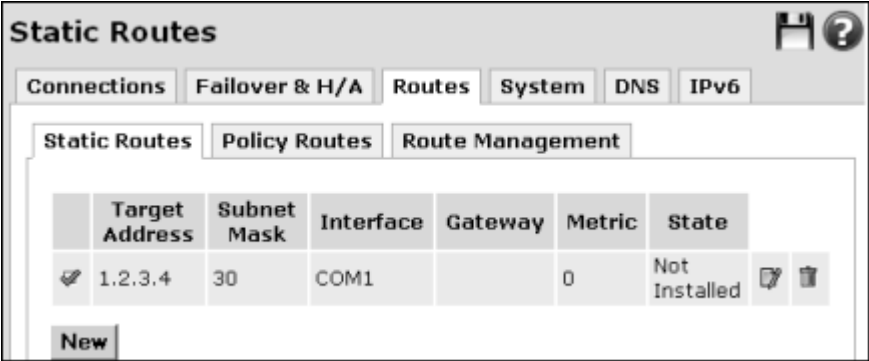
- 2 Click **New**. The Static Routes edit page appears.

Figure 107: Static Routes edit page



- 3 To add to the static route to the route table of the system, select the **Enable** check box. This check box is enabled by default.
- 4 [Required] Enter the IP address in the **Target Address** field.
- 5 [Required] Enter a value in the **Subnet mask** field that identifies the destination network or host. A subnet mask of 32 identifies a host route.
 - Accepted value range: A number between 0 and 32.
 - Can also be in the form 255.255.255.0.
- 6 [Optional] You can specify an Interface out which the network traffic should be routed from the **Interface** list. Only current, valid interface configurations can be selected. This field generally only needs to be specified if the target is directly connected to this appliance or if the target is on the remote end of a PPTP or L2TP link. Available options are:
 - None
 - Currently configured connections
- 7 [Optional] Enter a **Gateway Address** through which the network traffic should be routed.
- 8 [Required] Enter a value in the **Metric** field that represents the metric of this connection. This generally only has to be set if two or more routes conflict or have overlapping targets.
 - Accepted value range: A number equal to or greater than 0.
- 9 Click **Finish**.

Figure 108: Defined Static Routes

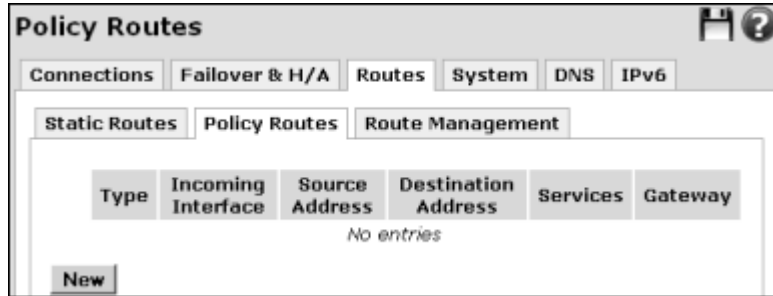


Policy Routes page

A policy route allows packets to be routed via a specific gateway based on their incoming interface, source address, destination address, and service.

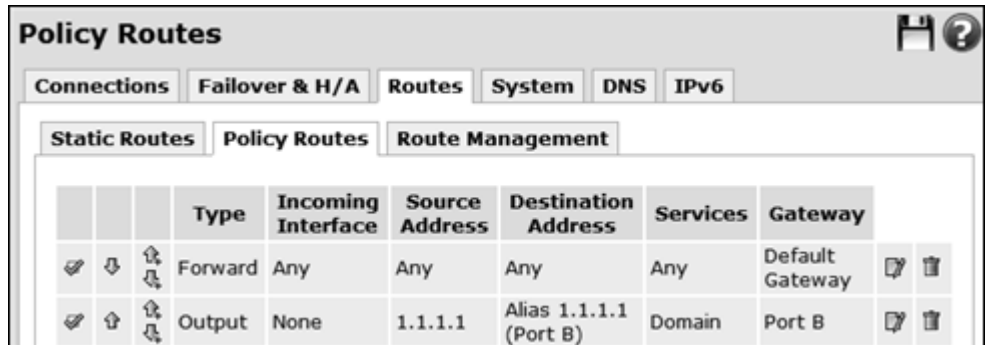
Click **New** to define the first route, as shown in Figure 109:

Figure 109: Policy Routes page — initial view



Thereafter, you can also use the add above or add below icon to add a route above or below an existing route. If you use the New button, the route is added to the bottom of the list. Use the up or down arrows to reposition a route. For more information on icons, see “Interface icons” on page 24. Once the page is populated with routes, you can edit and delete the routes as necessary.

Figure 110: Policy Routes page — populated view



Important: Routes are evaluated from top to bottom as displayed on the page. The first matching route determines the gateway for the packet, so the order of routes is important. To reorder a route, click the move up or down arrows.

Creating a policy route

Use this procedure to create a new policy route.

- 1 From the **Network Setup** menu, click **Network Setup > Routes tab > Policy Routes** tab. The Policy Routes page appears.
- 2 If this is the first route, click **New**. Otherwise, you can click the add above or below icon to add the route in the location you want above or below an already defined route. The Edit Policy Route page appears.

Figure 111: New Policy Routes

The screenshot shows the 'Edit Policy Route' dialog box. It features a tabbed interface with 'Connections', 'Failover & H/A', 'Routes', 'System', 'DNS', and 'IPv6'. The 'Routes' tab is selected, and within it, the 'Policy Routes' sub-tab is active. The configuration area contains several fields: 'Enable' is checked; 'Type' is set to 'Forward'; 'Incoming Interface' is set to 'Any'; 'Source Address' is set to 'Any' with a 'New' button; 'Destination Address' is set to 'Any' with a 'New' button; 'Services' is set to 'Any' with a 'New' button; and 'Gateway' is set to 'Default Gateway'. At the bottom, there are 'Finish' and 'Cancel' buttons.

- 3 Select the **Enable** check box.
- 4 From the **Type** list, select the type of policy route, which controls whether the incoming interface options are available. Available options are:
 - **Forward:** Select **Forward** to route forwarded packets only (with this option you can select the incoming interface).
 - **Output:** Select **Output** to route packets generated by this appliance (you cannot select the incoming interface with this option set)
- 5 Enter the **Incoming Interface** address that this appliance received the packet on, you can also select **Any** (to match packets received on any interface, but do not match packets generated by this appliance), or **None** (only match packets generated by this appliance).
- 6 Enter the **Source Address** that matches the source IP address of the packet. When you click **New**, you can create an address definition when you create this route.
- 7 Enter the **Destination Address** that matches the destination IP address of the packet. When you click **New**, you can create an address definition when you create this route.

- 8 Select the **Services** of the packet. If the service you require is not listed, click **New** to create it.
- 9 From the **Gateway** list, select the Internet connection to use as the gateway. If the Internet connection is not active, then the policy route has no effect. If you select the Default Gateway option, the route causes the packet to not be policy routed by subsequent policy routes.
- 10 Click **Finish**.

Enabling route management

Note: Route management does not have full Web management console configuration support. It is recommended that only advanced users familiar with the Zebra routing daemon and the RIP, BGP, or OSPF routing protocol attempt configuration of this feature.

Advanced users can configure the SnapGear appliance to automatically manage its routing tables, exchanging routes with other routers using RIP, BGP, or OSPF protocol.

- 1 From the **Network Setup** menu, click **Routes > Static Routes** tab.

Figure 112: Route Management page

- 2 Select the **Enable route management** check box.
- 3 Select the desired protocol from the **Protocol** list. Available options are:
 - BGP
 - OSPF
 - RIP (v1, v2)
- 4 Click **Update**.

The routing manager must now be configured manually by editing the appropriate configuration files.

Manually configuring route management

- 1 From the **System** menu, click **Advanced > Configuration Files** tab.
- 2 Select the check boxes for the `zebra.conf` and `protocol.d.conf` configuration files (for example, `ripd.conf`).
- 3 Click **Modify**.

A relatively trivial example for each protocol follows. You should not rely on these guides to configure route management for your network. Refer to the Zebra Web site (<http://www.zebra.org>) for comprehensive documentation.

Example: Configuring RIP Route Management

Ensure you have enabled **RIP(v1, v2)** under **Route Management**, then open **zebra.conf** and **ripd.conf** for editing as described in “Manually configuring route management” on page 144.

RIP version 2 is used by default.

! and **#** are comment characters. If the first character of the word is a comment character, the rest of the line forward is ignored as a comment. For example:

```
! password zebra
```

If a comment character is not the first character of the word, it is read as a normal character. In the example below, the **!** (exclamation mark) is not regarded as a comment and the password is set to **zebra!password**:

```
password zebra!password
```

In these examples, **!** denotes a descriptive comment and pound (**#**) indicates a configuration line that is currently commented out, which you may want to uncomment depending on your network setup.

In **zebra.conf**, enter:

```
! Uncomment and set telnet/vty passwords to enable telnet  
access on port 2601  
#password changeme  
#enable password changeme  
  
! Uncomment no multicast if you don't want to accept or  
send multicast rip packets for the specified interface  
#interface eth0  
#no multicast  
#interface eth2  
#no multicast
```

In `ripd.conf`, enter:

```
! Uncomment and set telnet/vty passwords to enable
telnet access on port 2602
#password changeme
#enable password changeme

! RIP version 2 authentication
#interface eth0
#ip rip authentication mode text
#ip rip authentication string snapgear

! Enable the RIP routing process
router rip
! Define interfaces which exchange RIP messages over
network eth0
#network eth2
! Define neighbor routers to exchange RIP with if
disabling multicast above in zebra.conf, or neighbors
don't have multicast enabled
#neighbor 192.168.45.238
#neighbor 192.168.45.231
! Redistribute routing information for interfaces with
RIP disabled
redistribute connected
! Redistribute routing information from static route
entries
redistribute static
! Redistribute routing information from kernel route
entries e.g. IPSec
redistribute kernel
```

The above files configure the device to listen for and send multicast RIP messages on the eth0 (LAN port) interface. You can see the above example has commented out additional interfaces which to exchange RIP messages over and optional neighbors routers to exchange RIP messages with if these neighbors can't accept multicast packets. There is also an example for setting up RIP version 2 authentication. Uncomment and configure as required.

Restart route management to enable the updated configuration – clear the **Enable route management** check box, click **Update**, select the **Enable route management** check box again and click **Update**.

If you prefer, you can uncomment the **password** and **enable password** lines, and then telnet to the relevant ports to configure Zebra and/or ripd via the

command line. The command line interface is very similar to the Cisco IOS interface. If you are familiar with this, you may prefer to configure using this method.

Example: OSPF

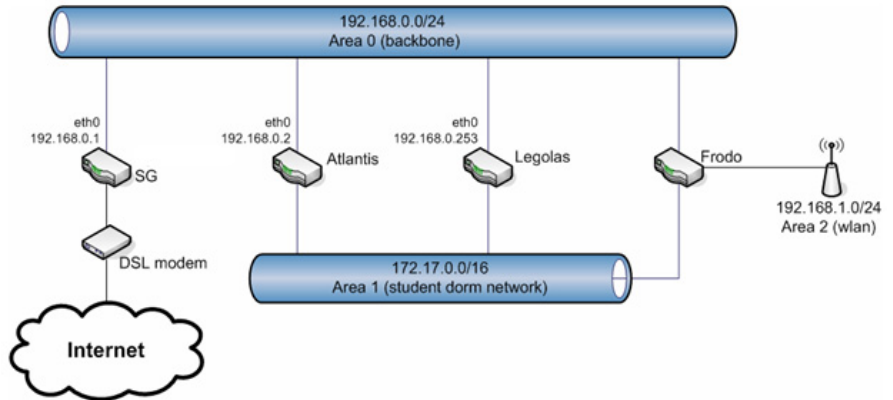
OSPF stands for Open Shortest Path First, and some of its principal features as follows:

- Networks are grouped by *areas*, which are interconnected by a *backbone area* which will be designated as *area 0*. All traffic goes through area 0, and all the routers in area 0 have routing information about all the other areas.
- Routes are propagated very fast, compared with RIP, for example.
- OSPF uses multicasting instead of broadcasting, so it doesn't flood other hosts with routing information that may not be of interest for them, thus reducing network overhead. Also, *Internal Routers* (those which only have interfaces in one area) don't have routing information about other areas. Routers with interfaces in more than one area are called *Area Border Routers*, and hold topological information about the areas they are connected to.
- OSPF is based on Dijkstra's Shortest Path First algorithm, which is CPU-intensive compared to other routing algorithms.
- OSPF counts with the special characteristics of networks and interfaces, such as bandwidth, link failures, and monetary cost.

This example is adapted from the LARTC (Linux Advanced Routing & Traffic Control) dynamic routing howto, available from: <http://lartc.org/howto/>. LARTC is an invaluable resource for those wanting to learn about and take advantage of the advanced routing capabilities of Linux systems.

In this example, route management is set up using OSPF for the network topology described by the following diagram:

Figure 113: OSPF network example



The SG is configured to exchange routes with the routers named *Atlantis*, *Legolas* and *Frodo*.

- 1 Ensure you have enabled **OSPF** under **Route Management**, then open **zebra.conf** and **ospfd.conf** for editing as described in “Manually configuring route management” on page 144.

- 2 In **zebra.conf**, enter:

```
hostname sg
! Uncomment and set telnet/vty passwords to enable telnet
access on port 2602
#password changeme
#enable password changeme

# Enable multicast for OSPF
interface eth1
multicast

! Example static default route for Internet connection
#ip route 0.0.0.0/0 212.170.21.129
```

- 3 In **ospfd.conf**, enter:

```
hostname sg
! Uncomment and set telnet/vty passwords to enable telnet
access on port 2604
#password changeme
#enable password changeme

! Instruct ospfd about our network topology
router ospf
network 192.168.0.0/24 area 0
network 172.17.0.0/16 area 1
```

- 4 Restart route management to enable the updated configuration – clear the **Enable route management** check box, click **Update**, select the **Enable route management** check box again and click **Update**.

If you prefer, you can uncomment the **password** and **enable password** lines, and then telnet to the relevant ports to configure Zebra or `ospfd` via the command line.

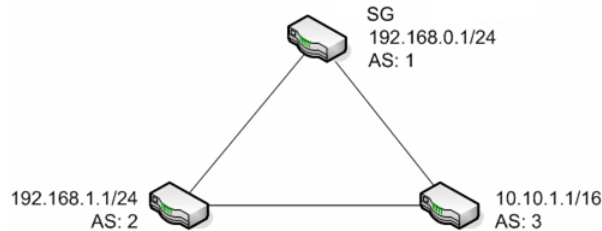
Example: BGP

This example is adapted from the LARTC (Linux Advanced Routing & Traffic Control) dynamic routing howto, available from: <http://lartc.org/howto/>. LARTC is an invaluable resource for those wanting to learn about and take advantage of the advanced routing capabilities of Linux systems.

The Border Gateway Protocol (BGP) allows the distribution of reachability information, that is, routing tables, to other BGP-enabled nodes. It can be used either as EGP or IGP. In EGP mode, each node must have its own Autonomous System (AS) number. BGP supports Classless Inter Domain Routing (CIDR) and route aggregation (merge multiple routes into one).

The following network map is used for this example. AS 2 and 3 have more neighbors but we need to configure only 2 and 3 as our neighbor.

Figure 114: BGP example network



Important: The AS numbers used in this example are reserved. Obtain your own AS from RIPE if you set up official peerings.

Ensure you have enabled **BGP** under **Route Management**, then open **zebra.conf** and **bgpd.conf** for editing as described in “Manually configuring route management” on page 144.

In **zebra.conf**, enter:

```
hostname sg
! Uncomment and set telnet/vty passwords to enable
telnet access on port 2602
#password changeme
#enable password changeme
```

In **bgpd.conf**, enter:

```
hostname sg
! Uncomment and set telnet/vty passwords to enable telnet
access on port 2605
#password changeme
#enable password changeme
```

```
! Access list, used to limit the redistribution to
private networks (RFC 1918)
access-list local_nets permit 192.168.0.0/16
access-list local_nets permit 172.16.0.0/12
access-list local_nets permit 10.0.0.0/8
access-list local_nets deny any

! Our AS number
router bgp 1
! Our IP address
bgp router-id 192.168.0.1
! Announce our own network to other neighbors
network 192.168.0.0/24
! Advertise all connected routes (directly attached
interfaces) redistribute connected
! Advertise kernel routes (manually inserted routes,
IPSec)
redistribute kernel
! Every 'router bgp' block contains a list of neighbors to
which the router is connected:
neighbor 192.168.1.1 remote-as 2
neighbor 192.168.1.1 distribute-list local_nets in
neighbor 10.10.1.1 remote-as 3
neighbor 10.10.1.1 distribute-list local_nets in
```

Restart route management to enable the updated configuration – clear the **Enable route management** check box, click **Update**, select the **Enable route management** check box again and click **Update**.

If you prefer, you can uncomment the **password** and **enable password** lines, and then telnet to the relevant ports to configure Zebra and/or ospfd via the command line. The command line interface is very similar to the Cisco IOS interface. If you are familiar with this, you may prefer to configure using this method.

System tab

The system device settings control the identity of the SnapGear appliance on the network. Use the Device Settings page to specify some basic system settings for the appliance.

Entering device settings

Use this procedure to set the hostname and other identifying information for the appliance.

The **Administrative Contact** and **Device Location** settings are used by the **SNMP** page in the **System** menu > **Management** menu option. For more information, see “Management menu” on page 486 and “Enabling the SNMP agent” on page 495.

The **Serial Number** field displays in the **System** menu **Diagnostics** page, and also in the Technical Support Report. For more information, see “System tab” on page 497 and “Technical Support Report page” on page 28. It is required to enable TrustedSource. See “Enabling TrustedSource” on page 342.

- 1 From the **Network Setup** menu, click **Network Setup** > **System** tab. The Device Settings page appears.

Figure 115: System tab — Device Settings page

The screenshot shows the 'Device Settings' page within a web interface. At the top, there are tabs for 'Connections', 'Failover & H/A', 'Routes', 'System' (which is selected), 'DNS', and 'IPv6'. Below the tabs, the 'Device Settings' section contains several form fields: 'Hostname' with the value 'SG565-tech-pubs', 'Workgroup' with 'SCUR', 'Administrative Contact' with 'sgadmin@mycompany.com', 'Device Location' with 'Brisbane', and 'Serial Number' with '0601860230330552'. A 'Submit' button is located at the bottom left of the form area.

- 2 Enter a descriptive name for the SnapGear appliance in the **Hostname** field. The hostname displays in the title bar of the browser, which identifies the appliance you are administrating. By default, this is set to the model name of your appliance; for example, *SG565*. This entry is also used as the SNMP *sysName* field. This name also displays when browsing the network from a Windows PC (*SG565 only*). A hostname must begin with an alpha character, and can consist of alphanumeric characters and hyphens.
- 3 [SG565 only] Enter the name of your Windows workgroup to which the appliance belongs in the **Workgroup** field. This field associates the appliance with a logical group of hosts that also have the same workgroup name. The Workgroup name displays in My Network Places in Windows Explorer.
 - Can be 1 or more characters of any type
 - Typically UPPERCASE
- 4 [Optional] Enter the email address of the local administrator of the SnapGear appliance in the **Administrative Contact** field. This entry is also for use as the SNMP *sysContact* field. This field can consist of any characters.
- 5 [Optional] Enter a short description of the physical location of the SnapGear appliance in the **Device Location** field. This entry is also for use as the SNMP *sysLocation* field. This field can consist of any characters.
- 6 [Recommended, required for TrustedSource] Enter the hardware serial number of the SnapGear appliance in the **Serial Number** field. The serial number is on a label located on the underside of the device. If this field is blank (not auto-populated), enter the serial number so it is readily available if you need to contact technical support. The serial number displays within the **System** menu > **Diagnostics** page and on the technical support report.
 - Must be exactly 16 digits (0-9)
- 7 Click **Submit**.

DNS

The DNS (Domain Name System) is a service that translates, or *maps*, host names to IP addresses. DNS also maps from IP address numbers to the machine name, which is referred to as *reverse mapping*. The DNS settings control the network name services of the SnapGear appliance. The DNS tab contains the following subtabs:

- “DNS Proxy tab”
- “Dynamic DNS tab” on page 155
- “Static Hosts tab” on page 160

The DNS configuration information is stored in `/etc/config/dnsmasq.conf`. For a complete list of options that can be stored in this file, run the following command from the command line interface:

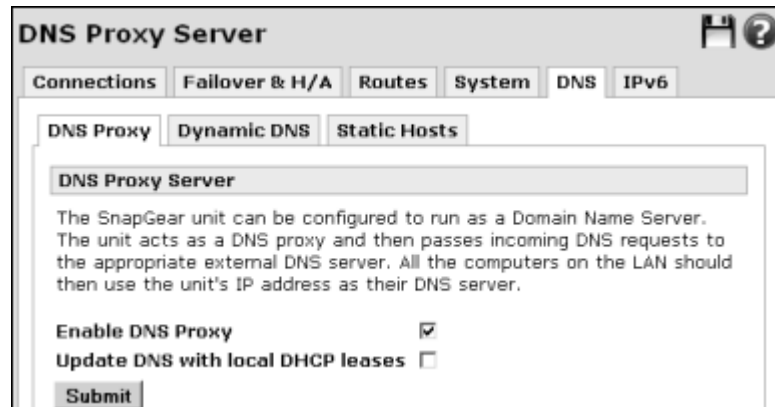
```
# dnsmasq --help
```

DNS Proxy tab

Use this tab to configure the SnapGear appliance to run a Domain Name Server (DNS) proxy. In the default configuration for DNS, the appliance passes incoming DNS requests from internal clients to an external DNS server, and forwards the reply back to the internal client. When the DNS proxy is enabled, all the computers on the LAN can specify the IP address of the SnapGear appliance as their DNS server. The DNS Proxy is enabled by default.

The DNS Proxy Server page is shown in Figure 116:

Figure 116: DNS Proxy Server page



Tip: For enhanced HTTP and FTP performance, enable Web caching for Internet requests. For information, see “Web cache” on page 176.

Enabling DNS proxy server

- 1 From the **Network Setup** menu, click **Network Setup > DNS > DNS Proxy** tab. The DNS Proxy Server page appears.
- 2 [Enabled by default] To enable the DNS Proxy and allow caching of DNS requests, select the **Enable DNS Proxy** check box. DNS caching is especially useful for improving response time when Internet access is through dialup, cable modem, or ADSL.
- 3 [Optional if using DHCP server] To enable forward and reverse lookups for hosts with DHCP leases from the SnapGear appliance, select the **Update DNS with local DHCP leases** check box. For information on configuring DHCP, see “DHCP Server” on page 162.
- 4 Click **Submit**.

Disabling DNS proxy server

- 1 From the **Network Setup** menu, click **Network Setup > DNS > DNS Proxy** tab. The DNS Proxy Server page appears.
- 2 Clear the **Enable DNS Proxy** check box.
- 3 Click **Submit**.

Dynamic DNS tab

Use this tab to configure a dynamic DNS account. If the Internet interface of the SnapGear appliance obtains its IP address using DHCP, Dynamic DNS can be used. A dynamic DNS service is useful when you do not have a static IP address but still require to remain contactable by hosts on the Internet. Dynamic DNS service providers such as TZO.com and dyndns.org can register an Internet domain name that points to your IP address no matter how often it changes. Whenever its Internet IP address changes, the SnapGear appliance alerts the dynamic DNS service provider and the domain name records are updated appropriately.

Prerequisite:Create an account with the supported dynamic DNS service provider of your choice.

The dynamic DNS providers currently supported by the SnapGear appliance are as follows:

- 3322.org (Chinese provider, <http://www.3322.org>)
- DyNS (<http://www.dyns.cx>)
- dyndns.org (<http://www.dyndns.org>)
- GNUDip (<http://gnudip.cheapnet.net>)
- ODS (<http://www.ods.org>)
- TZO (<http://www.tzo.com>)

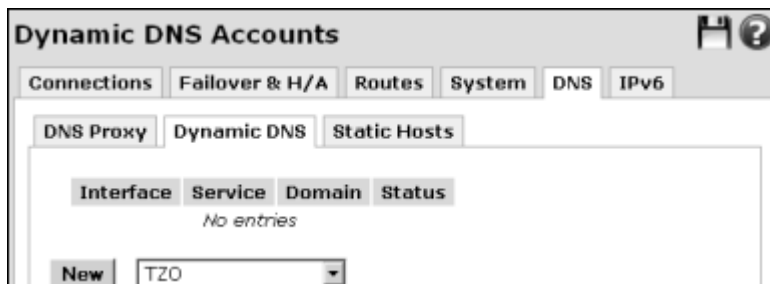
This section contains the following topics:

- “Creating a dynamic DNS account” on page 156
- “Disabling a dynamic DNS account” on page 159
- “Editing a dynamic DNS account” on page 159
- “Deleting a dynamic DNS account” on page 159

Creating a dynamic DNS account

- 1 From the **Network Setup** menu, click **Network Setup > DNS tab > Dynamic DNS** tab. The Dynamic DNS Accounts page appears.

Figure 117: Dynamic DNS Accounts page



- 2 Select the Dynamic DNS provider with whom you have an account from the list of supported providers. The dynamic DNS providers currently supported by the SnapGear appliance are as follows:
 - **3322.org**
 - **DyNS**
 - **dyndns.org**—Use this option if your dynamic DNS hostname is on the standard dyndns.org domains.
 - **dyndns.org (Custom)**—Use this option if your dynamic DNS hostname is on your own domain name that you own and have delegated to dyndns.org.
 - **GnuDip**
 - **ODS**
 - **TZO**
- 3 Click **New**. The Dynamic DNS page appears.

Figure 118: Define New Dynamic DNS

Dynamic DNS Accounts

Connections | Failover & H/A | Routes | System | **DNS** | IPv6

DNS Proxy | **Dynamic DNS** | Static Hosts

Service: dyndns.org

Enable: ☒

Interface: Default Gateway Interface

Username:

Password:

Confirm Password:

Domain:

Additional Domains:

MX:

Wildcard: ☒

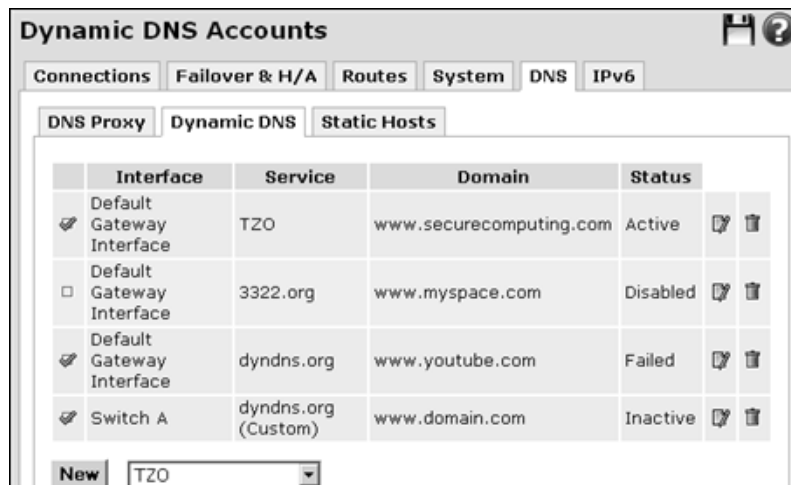
Finish Cancel

- 4 The **Enable** check box is selected by default. If you do not want to enable the account at this time, clear the **Enable** check box.
- 5 Select the port that you want associated with your newly created DNS account from the **Interface** list. The interface is the network connection you want to associate with the dynamic DNS account.

Tip: If you have multiple Internet connections, select **Default Gateway Interface** to use the current default gateway interface.

- 6 Enter the email address (your username) associated with your dynamic DNS account in the **E-mail Address** field.
- 7 Enter the password for your dynamic DNS account in the **Key** field.
- 8 Enter the domain for your dynamic account in the **Domain** field.
- 9 [Optional for **dyndns.org** provider only] If you have additional domains for this account, enter them with comma separators in the **Additional Domains** field.
- 10 [Optional for **dyndns.org** and **3322.org** providers only] To set the Mail eXchanger field for your dynamic DNS account, enter the hostname to point the MX records to in the **MX** field.
- 11 [Optional for **dyndns.org** and **3322.org** providers only] To set the wildcard option for your dynamic DNS account, select the **Wildcard** check box. The wildcard options updates all records attached to the dynamic DNS provider account, in addition to the record specified in the **Domain** field.
- 12 Click **Finish**. The account is added to Dynamic DNS Accounts page.

Figure 119: Dynamic DNS
Accounts page—Status



The screenshot shows the 'Dynamic DNS Accounts' page with tabs for Connections, Failover & H/A, Routes, System, DNS, and IPv6. Under the DNS tab, there are sub-tabs for DNS Proxy, Dynamic DNS, and Static Hosts. The Dynamic DNS tab is active, displaying a table with columns: Interface, Service, Domain, and Status. Below the table is a 'New' button and a dropdown menu showing 'TZO'.

Interface	Service	Domain	Status
<input checked="" type="checkbox"/> Default Gateway Interface	TZO	www.securecomputing.com	Active
<input type="checkbox"/> Default Gateway Interface	3322.org	www.myspace.com	Disabled
<input checked="" type="checkbox"/> Default Gateway Interface	dyndns.org	www.youtube.com	Failed
<input checked="" type="checkbox"/> Switch A	dyndns.org (Custom)	www.domain.com	Inactive

New

This page also displays the current **Status** for each dynamic DNS service. The status can be one of the following:

- **Active**—This service is enabled, and either has updated the IP address, or is currently updating the IP address.
- **Inactive**—This service is enabled, but the Interface is currently inactive.
- **Failed**—The previous attempt to update the IP address had a critical failure. You must edit the settings for this service and enter the correct details. See “Editing a dynamic DNS account” on page 159.
- **Disabled**—You have manually disabled this service. See “Disabling a dynamic DNS account” on page 159.

When you first define or re-enable a Dynamic DNS Service account, the **Status** is displayed as **Inactive**. Once you refresh your browser, the **Status** is displayed as **Active** or **Failed**.

Disabling a dynamic DNS account

- 1 From the **Network Setup** menu, click **Network Setup > DNS tab > Dynamic DNS** tab. The Dynamic DNS Accounts page appears.
- 2 Clear the enable check box next to the account you want to disable. The check mark is no longer displayed, and the **Status** column now displays **Disabled** without the need to refresh your browser.

Editing a dynamic DNS account

- 1 From the **Network Setup** menu, click **Network Setup > DNS tab > Dynamic DNS** tab. The Dynamic DNS Accounts page appears.
- 2 Click the edit icon for the account you want to edit. The Dynamic DNS edit page appears.
- 3 Make your changes and click **Finish**.

Deleting a dynamic DNS account

- 1 From the **Network Setup** menu, click **Network Setup > DNS tab > Dynamic DNS** tab. The Dynamic DNS Accounts page appears.
- 2 Click the delete icon for the account you want to delete. You are prompted to confirm the delete. Click **OK**.

Static Hosts tab

Use the Static Hosts tab to create, edit, and delete static hostnames. Static hostnames can be resolved to IP addresses on the SnapGear appliance even when DNS is not available. The static hostnames are stored in the `/etc/config/hosts` file. The DHCP server reserved hosts list is also stored in the hosts file, but do not display in the Static Hosts list.

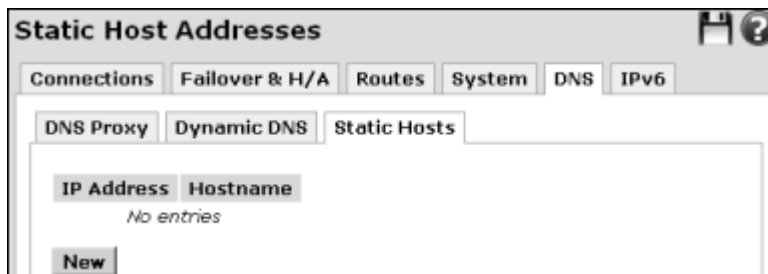
This section contains the following topics:

- "Creating a static host"
- "Editing a static host" on page 161
- "Deleting a static host" on page 161

Creating a static host

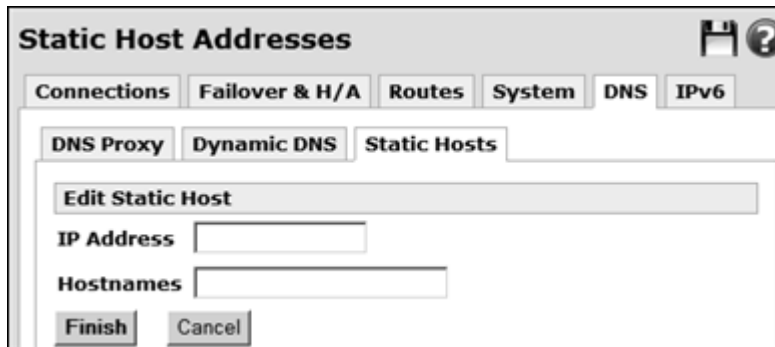
- 1 From the **Network Setup** menu, click **Network Setup > DNS > Static Hosts** tab. The Static Hosts page appears.

Figure 120: Static Hosts page



- 2 Click **New**. The Edit Static Hosts page appears.

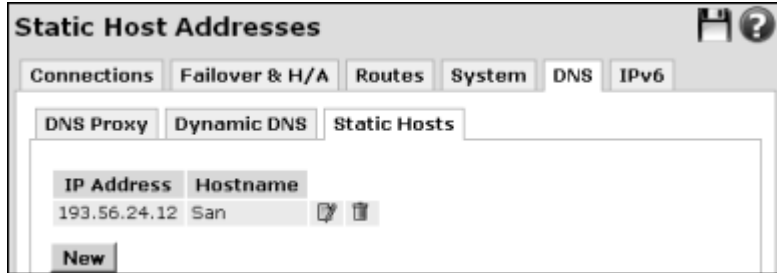
Figure 121: Edit Static Host page



- 3 Enter the IP address of the static host in the **IP Address** field.
- 4 Enter one or more hostnames that resolve to the Static Host IP address in the **Hostnames** field. Multiple hostname must be separated by spaces. Fully-qualified domain names are also accepted.

- 5 Click **Finish**. The Static Host information is displayed in the edit list.

Figure 122: Defined Static Host



Editing a static host

- 1 From the **Network Setup** menu, click **Network Setup > DNS > Static Hosts** tab. The Static Hosts page appears.
- 2 Select the edit icon for the static host you want to edit. The Edit Static Hosts page appears.
- 3 Make your changes and click **Finish**.

Deleting a static host

- 1 From the **Network Setup** menu, click **Network Setup > DNS > Static Hosts** tab. The Static Hosts page appears.
- 2 Select the delete icon for the static host you want to delete. You are prompted to confirm the delete. Click **OK**.

DHCP Server

DHCP (Dynamic Host Configuration Protocol) is used for assigning dynamic IP address to devices on a network. IP addresses are assigned using the concept of a *lease*, which is the amount of time the IP address is valid for a device. With DHCP, network administrators can centrally manage and automate the assignment of IP addresses. DHCP is only available for non-Internet interfaces, such as LAN or DMZ, defined with static IP addresses.

Note: *If an interface itself is defined to use DHCP, that interface cannot act as a DHCP Server or Relay.*

You can set up the appliance as either a DHCP Server or a DHCP Relay. When the appliance is configured as a DHCP server, it assigns addresses for a particular IP address space. When the appliance is configured as a DHCP relay, the appliance is configured with the IP address of a DHCP server.

If the DHCP server resides on another network (that is, the DHCP Server and the client network are on opposite sides of a router, it is necessary to set up a DHCP relay since DHCP broadcasts cannot be passed by the router. DHCP Relay packets have a source and destination IP address; however, DHCP relay does not support NAT. If the DHCP server and client reside on the same side of a network, set up a DHCP server. A DHCP server can reside on a different network than the client network. For example, the DHCP server can have an IP address of 10.10.1.254 and assign addresses in the 192.168.0.0 network.

DHCP is defined by RFC2131. For details, visit the following URL:
<http://www.faqs.org/rfcs/rfc2131.html>.

The main pages for DHCP in the Web management console are as follows:

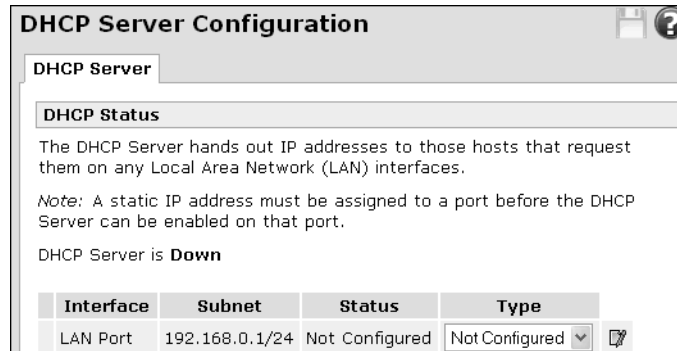
- “DHCP Status page” on page 163
- “DHCP Addresses page” on page 167
- “DHCP Relay page” on page 171

DHCP Status page

Use this page to view the status of the DHCP server, and to configure an interface as a DHCP server or relay. To access this page, from the **Network Setup** menu, click **DHCP Server**. The DHCP status page appears.

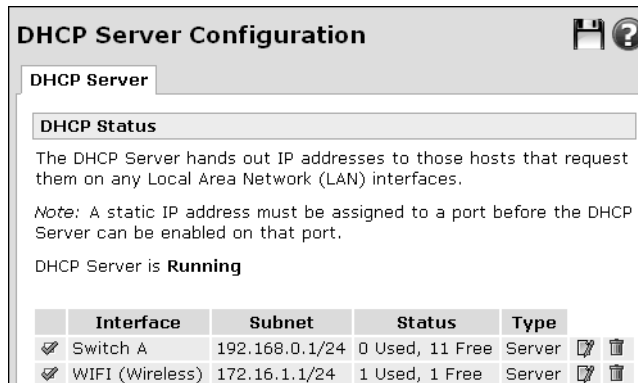
To begin configuring a server or relay, select the option you want from the **Type** list. The initial view of this page is **Not Configured** for **Status** and **Type**. The status message “DHCP Server is Down” is displayed. Figure 123 shows the initial view of this page:

Figure 123: DHCP Server—Not Configured



Once a DHCP Server or Relay is configured, this main DHCP server page displays the status for each interface on which the DHCP server is running, and the status message “DHCP Server is Running” is displayed. Figure 124 shows a configured and running view of this page:

Figure 124: DHCP Server Status—Configured and Running



Important: If the **Free** value is 0 (zero), all of the available IP addresses are taken. Increase the number of IP addresses to distribute. See “Adding a dynamic IP address or range” on page 169.

You can disable and enable the configuration in the leftmost column. The **Interface** column displays the interface for which the DHCP server or relay is configured. The **Subnet** column contains the network on which the DHCP server is handing out addresses. The **Status** column displays the number of Used and Free IP addresses for distribution. The **Type** column indicates whether the DHCP is configured as a server or a relay. The edit and delete icons become available after an interface is configured as a DHCP server or relay.

Configuring a DHCP server

Use this procedure to configure a DHCP server for an interface.

Note: To configure your SnapGear appliance as a DHCP server, you must set a static IP address and netmask on the network interface on which you want the DHCP server to run. For more information, see “Direct connection overview” on page 38.

- 1 From the **Network Setup** menu, click **DHCP Server**. The DHCP Server Configuration page appears.
- 2 For the interface you want to configure, select **DHCP Server** from the **Type** list. The Server Configuration page appears.

Figure 125: DHCP Server Configuration

Server Configuration	
Interface	LAN Port
Subnet	192.168.0.1/24
Enable DHCP Server for this Subnet	<input checked="" type="checkbox"/>
Gateway Address	192.168.0.1
DNS Addresses	192.168.0.1
Domain Name	
WINS Addresses	
Default Lease Time (s)	86400
Maximum Lease Time (s)	172800
Address Range	

The **Interface** display only field indicates the interface you are about to configure to issue addresses as specified by the **Subnet** display field. In Figure 125, the **Interface** is the **LAN Port** and the **Subnet** is 192.168.0.1/24.

- 3 The **Enable DHCP Server for this Subnet** check box is selected by default. Clear the check box if you do not want the server enabled at this time.

- 4 Enter the IP address to issue the DHCP clients in the **Gateway Address** field. If this field is left blank, the IP address of the appliance is used. This field sets the default route.
- 5 Enter the IP address or addresses with which to configure a DNS server for DHCP clients in the **DNS Addresses** field. You can enter multiple addresses separated by spaces. You can usually leave this field blank, in which case the DNS server address is set as per the following:
 - If the DNS Proxy is enabled (default, see “DNS Proxy tab” on page 153), then the DNS server is set to the IP address of the network interface on which the DHCP server is listening.
 - If the DNS Proxy is disabled (see “Disabling DNS proxy server” on page 154), then the DNS server is set to all of the DNS servers used by the appliance. This typically includes the DNS servers that have been configured either manually or automatically for any connections (see “Connections” on page 35).
- 6 [Optional] Enter the name of the domain being configured in the **Domain Name** field. This sets the DNS suffix.
- 7 [Optional] Enter the IP address of the WINS server to be distributed to DHCP clients in the **WINS Addresses** field. You can enter multiple addresses separated by spaces.
- 8 In the **Default Lease Time** field, enter amount of time in seconds assigned to the lease if a DHCP client requesting the lease does not request a specific time to expire.
 - Default: 86400
- 9 In the **Maximum Lease Time** field, enter the maximum time in seconds that a dynamically assigned IP address is valid before the client must request it again.
 - Default: 172800
- 10 Enter the IP address range in the **Address Range** field. Addresses will be assigned to clients from within this range. Once you enter a range of address on this page, you must manage the addresses from that point onward in the DHCP Addresses page. For more information, see “DHCP Addresses page” on page 167.
- 11 Click **Finish**. The DHCP Server Status page reflects the new configuration and shows the number of used and free addresses. You can now click the edit icon to access the DHCP Addresses page.

Editing a DHCP server configuration

Use this procedure to edit a DHCP Server configuration. If you want to change the Type to DHCP Relay, you must delete the configuration first. See “Deleting a DHCP server or relay configuration” on page 167.

- 1 From the **Network Setup** menu, click **DHCP Server**. The DHCP Server Configuration Status page appears.
- 2 Click the edit icon for the Interface DHCP Server configuration you want to edit. The DHCP Addresses page appears for the Interface.
- 3 Click the **DHCP Configuration** tab. The Server Configuration page for the interface appears.
- 4 Make your changes and click **Update**. If you want to edit IP address ranges, you must now use the DHCP Address tab. See “DHCP Addresses page” on page 167.

Disabling a DHCP server or relay

Use this procedure to disable a DHCP server or relay.

Note: The procedure to configure a DHCP relay is located on page 171.

- 1 From the **Network Setup** menu, click **DHCP Server**. The DHCP Configuration page appears.
- 2 Clear the enable check box for the DHCP server or DHCP relay. The Status column changes from *m* Used, *n* Free to Disabled. Once you refresh your browser, the “DHCP Server is Running” message changes to “DHCP Server is Down”.

Re-enabling a DHCP server or relay

Use this procedure to enable a disabled a DHCP server or relay.

Note: The procedure to configure a DHCP relay is located on page 171.

- 1 From the **Network Setup** menu, click **DHCP Server**. The DHCP Configuration page appears.
- 2 Select the enable check box for the disabled DHCP server or DHCP relay. The **Status** column changes from **Disabled** to *m* Used, *n* Free. Once you refresh your browser, the “DHCP Server is Down” status message changes to “DHCP Server is Running.”

Deleting a DHCP server or relay configuration

Use this procedure to disable a DHCP server or relay.

Note: The procedure to configure a DHCP relay is located on page 171.

- 1 From the **Network Setup** menu, click **DHCP Server**. The DHCP Configuration page appears.
- 2 Click the delete icon for the DHCP Server or Relay configuration you want to delete. You are prompted to confirm the delete.
- 3 Click **OK**. The **Status** and **Type** list display **Not Configured**.

DHCP Addresses page

Note: This page becomes available after an interface has been configured as a DHCP server. See “Configuring a DHCP server” on page 164.

Use this page to view the status of IP addresses. You can also free leased addresses; and add, reserve, and delete addresses.

Figure 126: DHCP Addresses page

DHCP Server Configuration

DHCP Server

DHCP Configuration **DHCP Addresses**

Address List

Interface: WIFI (Wireless)
Subnet: 172.16.1.1/24

IP Address	Status	Hostname	MAC Address	Free
172.16.1.101	Reserved	SGadmin	00:18:DE:3C:BC:88	
172.16.1.102	Free			

Refresh

Add/Remove Dynamic IP Addresses

You may add or remove dynamic IP addresses for the DHCP server by specifying those addresses below. (Note: The IP address field will accept a range or a single IP address as input. For example: 192.168.0.234-238 or 192.168.0.1).

IP Address:

Add **Remove**

Add Reserved IP Addresses

You may add reserved IP addresses for the DHCP server by specifying their details below. Please enter in the MAC Address in the form AB:CD:EF:12:34:56.

Hostname:

MAC Address:

IP Address:

Submit

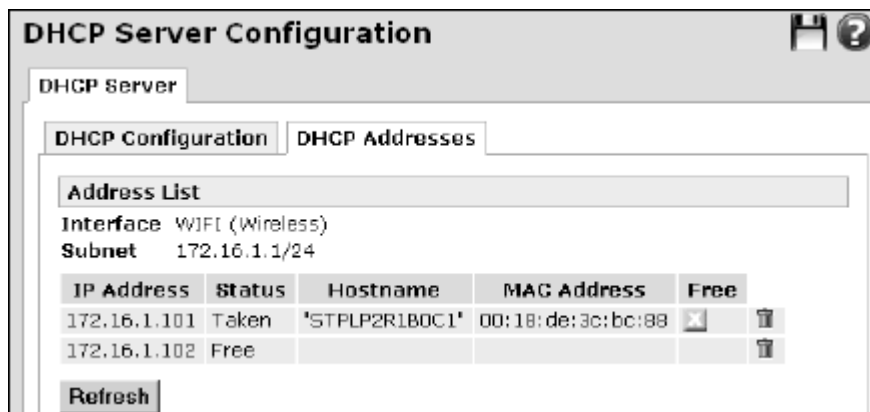
This page consists of three main panes:

- Address List pane
- Add/Remove Dynamic IP Addresses pane
- Add Reserved IP Addresses pane

Address List pane

Use this pane to view the status of the IP addresses the DHCP server is configured to distribute. Figure 127 shows the Address List pane of the DHCP Addresses page:

Figure 127: DHCP Addresses—Address List pane



The **Interface** and **Subnet** for the configuration are displayed. For each **IP Address** that the DHCP server is managing, the **Status**, **Hostname**, and **MAC Address** are displayed in the **Address List** pane. The **Status** column displays one of three states:


- **Reserved** — An address is reserved for the particular host defined by hostname and MAC address.
- **Free** — An address is available to be handed out to any DHCP client host.
- **Taken** — An address has been issued to a host.

Click **Refresh** to obtain the most current information. Click the delete icon to delete an IP address. If an address is taken by a client, a delete icon appears in the **Free** column so that you can free up an address in use.

Freeing a taken IP address

Use this procedure to free a leased IP address. A leased address has **Taken** displayed in its **Status** column. This causes the lease to expire immediately, leaving the address available for the next host that requests IP configuration.

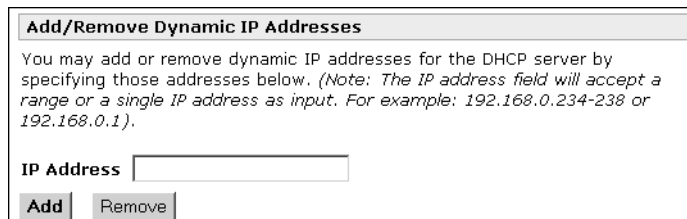
Note: A reserved address cannot be freed at this time. It must be deleted and added again.

- 1 From the **Network Setup** menu, click **DHCP Server**. The status page appears.
- 2 Click the edit icon for the Interface you want to edit. The DHCP Addresses page appears for the Interface.
- 3 In the **Address List** pane, click the free address  icon in the **Free** column for the address you want to release for use.

Add/Remove Dynamic IP Addresses pane

Use this pane to manually add or remove a dynamic IP address or address range. Figure 128 shows the Add/Remove Dynamic IP Addresses pane of the DHCP Addresses page:

Figure 128: DHCP Addresses—Add/Remove Dynamic IP Addresses pane



Add/Remove Dynamic IP Addresses

You may add or remove dynamic IP addresses for the DHCP server by specifying those addresses below. (Note: The IP address field will accept a range or a single IP address as input. For example: 192.168.0.234-238 or 192.168.0.1).

IP Address

Add **Remove**

Adding a dynamic IP address or range

- 1 From the **Network Setup** menu, click **DHCP Server**. The status page appears.
- 2 Click the edit icon for the Interface you want to edit. The DHCP Addresses page appears for the Interface.
- 3 In the **Add/Remove Dynamic IP Addresses** pane, enter the address or address range in the **IP Address** field.
- 4 Click **Add**. The address is added to the **Address List** pane.

Removing a dynamic IP address or range

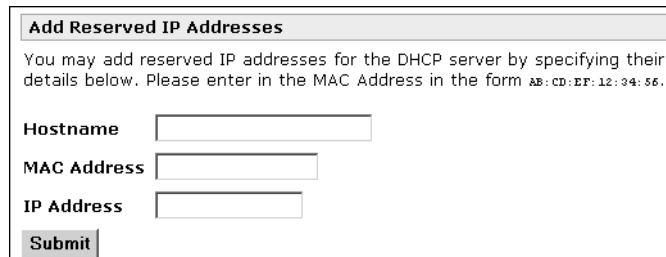
Tip: To quickly remove an address, click its delete icon in the **Address List** pane.

- 1 From the **Network Setup** menu, click **DHCP Server**. The status page appears.
- 2 Click the edit icon for the Interface you want to edit. The DHCP Addresses page appears for the Interface.
- 3 Under **Add/Remove Dynamic IP Addresses**, enter the IP address or IP address range you want to remove.
- 4 Click **Remove**. The address or addresses are removed from the **Address List** pane.

Add Reserved IP Addresses pane

Use this pane to reserve an IP address for a client based on their MAC address. Figure 129 shows the Add Reserved IP Addresses pane of the DHCP Addresses page:

Figure 129: DHCP Addresses—Add Reserved IP Addresses pane



Add Reserved IP Addresses

You may add reserved IP addresses for the DHCP server by specifying their details below. Please enter in the MAC Address in the form AB:CD:EF:12:34:56.

Hostname

MAC Address

IP Address

Submit

Reserving an IP address

Use this procedure to reserve an IP address to select clients based on their MAC address. You can reserve IP addresses for particular hosts, identifying them by hostname and MAC address. These reserved hosts are also added to the `/etcconfig/hosts` file (static hosts) for DNS purposes; for more on static hosts, see “Static Hosts tab” on page 160. Reserving an IP address allows computers on the LAN to use the names even if there is no other DNS server available. This is useful for sites that are too small to run a DNS/WINS server. Both the DHCP reserved hosts and the Static hosts configuration work together so that when you create a MyWebServer 10.0.0.5 machine, everyone on the internal network can ping and connect to it.

- 1 From the **Network Setup** menu, click **DHCP Server**. The status page appears.
- 2 Click the edit icon for the Interface you want to edit. The DHCP Addresses page appears for the Interface.

- 3 In the **Add Reserved IP address** pane, enter the following:
 - a Enter the **Hostname** of the DHCP client.
 - b Enter the **MAC Address** of the DHCP client.
 - c Enter the reserved **IP Address** for the DHCP client.
 - d Click **Submit**. The **Status** column of the address you reserved changes to **Reserved** in the **Address List** pane.

DHCP Relay page

Use this page to configure a DHCP relay on the selected interface. A DHCP relay allows you to forward DHCP requests to a DHCP server on another network. This allows you to use a single DHCP server to handle multiple networks. The DHCP proxy allows the SnapGear appliance to forward DHCP requests from the LAN to an external server for resolution. This allows both static and dynamic addresses to be given out on the LAN just as running a DHCP server would.

Note: DHCP relay does not support Network Address Translation (NAT).

The SnapGear appliance is configured with the IP address of the DHCP Server. The appliance accepts client DHCP Discover packets and relays them to the DHCP Server. The appliance returns information received from the DHCP Server back to the client.

Configuring a DHCP relay

- 1 From the **Network Setup** menu, click **DHCP Server**. The DHCP Status page appears.
- 2 From the **Type** list, select **Relay** for the interface you want to configure. The DHCP Relay page appears.

Figure 130: DHCP Server Relay page

The screenshot shows a window titled "DHCP Server Configuration" with a "DHCP Relay" tab selected. The configuration details are as follows:

Field	Value
Interface	LAN Port
Subnet	192.168.0.1/24
Enabled	<input checked="" type="checkbox"/>
Relay Server	

At the bottom of the window are two buttons: "Finish" and "Cancel".

- 3 The **Enabled** check box is selected by default.
- 4 In the **Relay Server** field, enter the IP address of a DHCP server located on another network.

5 Click **Finish**.

Editing a DHCP relay configuration

Use this procedure to edit a DHCP Relay configuration. You can enable or disable the relay, or change the IP address of the DHCP Relay server.

If you want to change the Type to DHCP Server, you must delete the configuration first before reconfiguring as a DHCP Server. See “Deleting a DHCP server or relay configuration” on page 167.

- 1** From the **Network Setup** menu, click **DHCP Server**. The DHCP Server Configuration Status page appears.
- 2** Click the edit icon for the Interface DHCP Relay configuration you want to edit. The DHCP Relay page appears.
- 3** Make your changes and click **Finish**.

Configuring the Windows client for DHCP

Use this procedure to set the TCP/IP properties for the LAN interface to obtain an IP address automatically. The Windows client must be configured if you have configured a DHCP Server or Relay. This procedure is for the Windows XP Professional operating system. You must have administrative rights to configure Windows XP as a DHCP client.

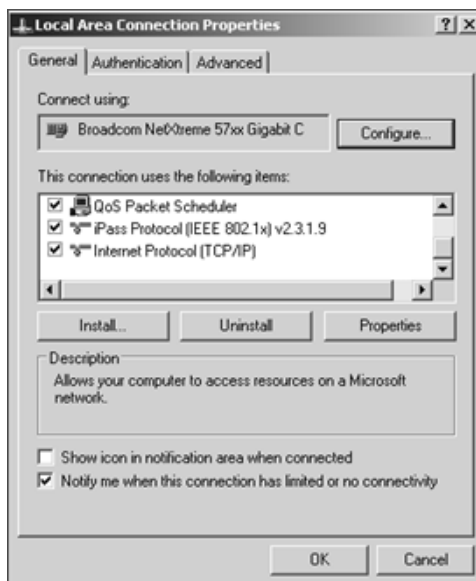
- 1 Click **Start > Settings > Network Connections > Local Area Connection**. The Local Area Connection Status dialog box appears.

Figure 131: Windows Local Area Connection Status dialog box



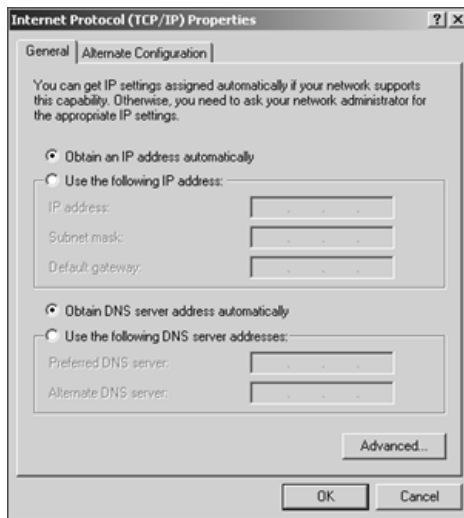
- 2 Click **Properties**. The Local Area Connection Properties dialog box is displayed.

Figure 132: Windows
Local Area Connection
Properties dialog box



- 3 Select **Internet Protocol (TCP/IP)** in the connection item list and click **Properties**. The Internet Protocol (TCP/IP) Properties dialog box appears.

Figure 133: Windows
Internet Protocol (TCP/IP)
Properties dialog box



- 4 Select **Obtain an IP address automatically**, **Obtain DNS server address automatically** and click **OK**, and **OK** again.

Verifying and troubleshooting DHCP

Once you have configured DHCP, verify that it is working correctly:

- Check the DHCP Server page to see if it has assigned any IP addresses.
- On the PC, verify that the PC has acquired an IP address using `ipconfig`.
- Use the `tcpdump` within the Web management console (see “Capturing and displaying packets” on page 506) or the command line interface to see DHCP packets. Look for the DHCP Discover packets:

```
20:14:03.401025 IP 0.0.0.0.68 > 255.255.255.255.67: UDP,  
length 302
```

Note that UDP port 67 is used for the DHCP server and UDP port 68 is used for the DHCP client.

- If the SnapGear appliance is being used as an DHCP client, inspect the front panel LEDs. If the appliance's LAN interface cannot get a DHCP-assigned IP address, all lights flash simultaneously. To remedy this:
 - Verify a valid Ethernet link on the LAN connection of the SnapGear appliance. To validate an Ethernet link, check the LEDs on the rear of the appliance. Ensure the Ethernet link LED is lit. For more information on the LEDs for a model, see the relevant LEDS topic in Chapter 1, Introduction.
 - Verify with the administrator of the DHCP server that it is running and contactable via broadcast on the SnapGear LAN interface.
 - Verify with the administrator of the DHCP server that there are free addresses available for clients.
- Inspect the system log for any errors.

Web cache

Note: Web Cache is applicable to SG565, SG580, SG640, and SG720 models only.

Web browsers running on PCs on your LAN can use the proxy-cache server of the SnapGear appliance to reduce Internet access time and bandwidth consumption. A proxy-cache server implements Internet object caching, which is a way to store requested Internet objects (that is, data available via HTTP, FTP, and other protocols) on a server closer to the user's network than on the remote site. Typically, the proxy-cache server eliminates the need to re-download Internet objects over the available Internet connection when several users simultaneously attempt to access the same Web site. The Web site's contents are available in the cache (server memory or disk) and are quickly accessible over the LAN rather than over the slower Internet link.

The Web cache keeps objects cached in memory and, on a LAN network share, caches Internet name (DNS) lookups and implements negative caching of failed requests. Using the lightweight ICP (Internet Cache Protocol), multiple Web caches can be arranged in a hierarchy or mesh. This mesh allows Web cache peers to pull objects from each other's caches, further improving the performance of Web access for an organization with multiple Internet gateways. The Web cache of the appliance can be configured to share cached objects with, and access objects cached by, other Web caches (peers). Web caches communicate using ICP. ICP is used to exchange hints about the existence of URLs in neighbor caches. Caches exchange ICP queries and replies to gather information to use in selecting the most appropriate location from which to retrieve an object. The messages transmitted by a cache to locate a specific object are sent to Sibling caches, which are placed at the same level in the hierarchy. Then, the caches placed at the Parent level are queried if the replies from sibling caches did not succeed. For information, see "Configuring Web Cache Peers" on page 185.

The Web cache can also be configured to pass off Web transaction requests or responses to a third-party ICAP server for processing, using its ICAP client. This is typically used to integrate a third-party virus scanning, content filtering, or a complete CSM solution, such as Webwasher. For information about ICAP, see "Configuring ICAP client for Web Cache" on page 186. For information about Webwasher content filtering, see "Enabling Webwasher content filtering" on page 319.

Enabling the Web cache

Use this procedure to enable the Web cache. Allocating auxiliary storage for the cache either on the network or locally is highly recommended. See “Allocating network storage for Web cache” on page 180 and “Allocating local USB storage for Web caching” on page 184.

The maximum amount of memory you can safely reserve depends on what other services the appliance has running, such as VPN or a DHCP server. If you are using a Network Share or Local Storage, it is generally best to set the Cache size to 8 Megabytes. Otherwise, start with a small cache (16 Megabytes) and gradually increase it until you find a safe upper limit where the appliance can still operate reliably.

PAC file

As the onscreen instructions indicate, users on the LAN must configure their browsers using the PAC (Proxy Automatic Configuration) file available at:

<http://192.180.0.1/proxy.pac>

Or, they can manually configure their proxy server settings to 192.168.0.1 on port 3128. For instructions, see “Configuring browsers to use the Web cache” on page 182.



Important: If you have any DMZ or Guest interfaces, non-LAN Bridges or multiple LAN interfaces, then the PAC file will not work unless the network users have their default gateway set to the IP address of this SnapGear appliance. In complicated network scenarios, you may need to manually edit the proxy.pac file for completeness and reliability.

Figure 134: Web Cache
— Main tab

The screenshot shows the 'Web Cache' configuration page with the 'Main' tab selected. The page has a title bar with 'Web Cache' and a help icon. Below the title bar are three tabs: 'Main', 'Storage', and 'Advanced'. The 'Main' tab is active and contains the following content:

- A section titled 'Web Cache' with a description: 'The web cache allows a limited number of web pages to be cached on the SnapGear unit. This could improve performance when several users attempt to access the same web site simultaneously.'
- A paragraph: 'Users on the LAN can either configure their web browsers using the Proxy Automatic Configuration file available here: <http://192.168.0.1/proxy.pac> or manually configure their proxy server settings to 192.168.0.1 on port 3128.'
- An 'Enable' checkbox, which is currently unchecked.
- A 'Cache size' dropdown menu set to '8 Megabytes'.
- A 'Submit' button.

- 1 From the **Network Setup** menu, click **Web Cache > Main** tab. The Web Cache page appears.
- 2 Select the **Enable** check box.
- 3 From the **Cache Size** list, select a cache size for memory (RAM) to reserve on the SnapGear appliance. Available options are: 1, 2, 4, 8, 12, 16, 20, 24, or 32 Megabytes.
- 4 Click **Submit**. Follow the instructions on the Web Cache page for configuring Web browsers. For details, see “Configuring browsers to use the Web cache” on page 182.

Disabling the Web Cache

- 1 From the **Network Setup** menu, click **Web Cache > Main** tab. The Web Cache page appears.
- 2 Clear the **Enable** check box.
- 3 Click **Submit**.

Creating a user account and network share in Windows XP

A network share is a shared folder or drive on a local Windows PC, or a PC running another operating system capable of SMB sharing (such as a Linux PC running the SAMBA service). Refer to the documentation of your particular operating system for details on creating a network share. This section includes basic procedures for creating a user account and network share under Windows XP. Refer to the Microsoft site for more detailed information.

Create a user account in Windows

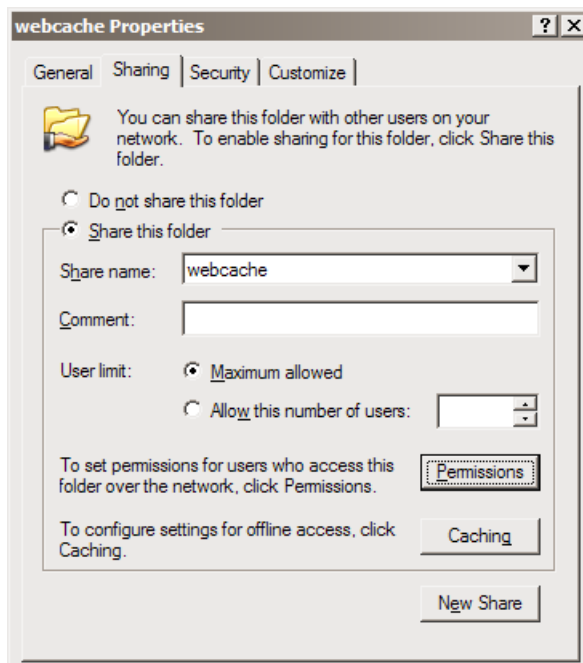
Use this procedure to create a user account in Windows XP for the Web cache. It is recommended a special user account is created for use by the SnapGear appliance for reading and writing to the network share. If you have an existing account or want to grant read and write access to everyone to the network share, skip this procedure.

- 1 Click **Start > Control Panel > User Accounts > Create a new account**.
- 2 Type a name for the new account, such as *sguser*, and click **Next**. Typically it is sufficient to grant this account **Limited** privileges.
- 3 Click **Create Account**.
- 4 Select the account you have just created under **Pick an account to change**.
- 5 Select **Create a password**. Enter and confirm a password for this account, as well as a password hint if desired.

Create a network share

Use this procedure to create a Network share in Windows XP for the Web cache.

Figure 135: webcache Properties



- 1 Launch Windows Explorer (**Start > (All) Programs > Accessories > Windows Explorer**) and open up a folder or drive to dedicate as a network share for use by the SnapGear appliance's Web cache.
- 2 Begin by disabling simple file sharing for this folder. From the **Tools** menu, select **Folder Options**. Click the **View** tab and under the **Advanced settings** section clear **Use simple file sharing (Recommended)**. Click **OK**.
- 3 Next, share the folder. Right-click the folder and select **Sharing and Security**. Select **Share this folder** and note the **Share name**. You can change this to something easier to remember if you want.
- 4 To set the security permissions of the newly created network share, click **Permissions**.
- 5 [Recommended] If you want to secure the network share with a user name and password, click **Add** and type the user name of the account to be used by the SnapGear appliance. Click **Check Names** and then click **OK**.
- 6 Select this account, or **Everyone** if you are not securing the network share with a user name and password, and check **Allow** next to **Full Control**. Click **OK** and **OK** again to finish.

Allocating network storage for Web cache

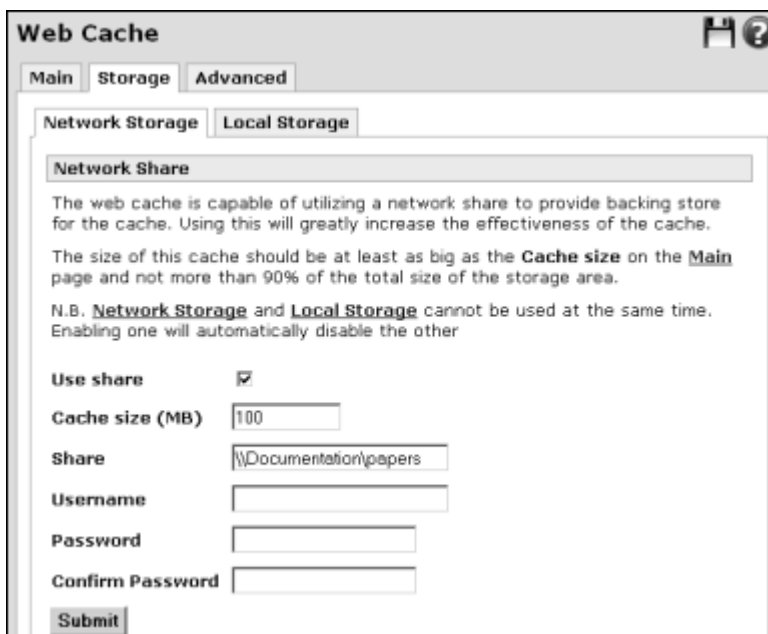
Use this procedure to configure network storage for Web cache.

Prerequisite: Create a network folder to share. See “Create a network share” on page 179.

If you prefer, you can use local USB storage (SG565 model only) instead of Network Storage. For more information, see “Allocating local USB storage for Web caching” on page 184.

- 1 From the **Network Setup** menu, click **Web Cache > Storage > Network Storage** tab. The Web Cache Network Storage page appears.

Figure 136: Network Storage (Web caching)



The screenshot shows the 'Web Cache' configuration window with the 'Storage' tab selected. Under the 'Storage' tab, the 'Network Storage' sub-tab is active. The page contains a 'Network Share' section with explanatory text and a form for configuration. The form includes a 'Use share' checkbox (checked), a 'Cache size (MB)' field (100), a 'Share' field (\\Documentation\papers), and fields for 'Username', 'Password', and 'Confirm Password'. A 'Submit' button is at the bottom.

Web Cache

Main Storage Advanced

Network Storage Local Storage

Network Share

The web cache is capable of utilizing a network share to provide backing store for the cache. Using this will greatly increase the effectiveness of the cache.

The size of this cache should be at least as big as the **Cache size** on the **Main** page and not more than 90% of the total size of the storage area.

N.B. **Network Storage** and **Local Storage** cannot be used at the same time. Enabling one will automatically disable the other

Use share ☒

Cache size (MB)

Share

Username

Password

Confirm Password

Submit

- 2 Select the **Use share** check box.
- 3 Enter the cache size in the **Cache Size** field. The size should be at least as big as the Cache size on the Main page and not more than 90% of the total size of the share.
- 4 Enter the path of the network share in the **Share** field using the following format:
`\\HOSTNAME\sharename`
- 5 If you allowed Full Control to Everyone on the network share drive, leave the Username and Password fields blank and go to the last step. Otherwise, if the dedicated user account must authenticate to the network share, continue with the next step.

- 6 Enter the username of the dedicated user in the **Username** field. The user must be able to read to and write from the network share.
- 7 Enter the password for authentication with the network share in the **Password** field.
- 8 Enter the password again in the **Confirm Password** field. The password field entries must match.
- 9 Click **Submit**. You can now configure personal computers on your LAN to use the Web cache. See "Configuring browsers to use the Web cache".

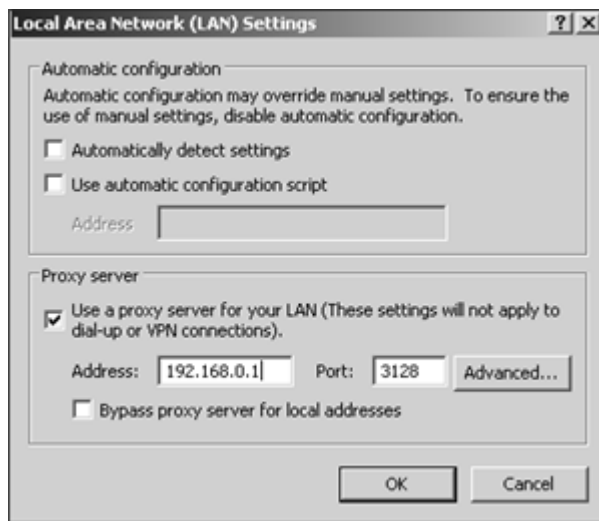
Configuring browsers to use the Web cache

Once the Web cache has been set up, personal computers on the LAN must have their browsers configured appropriately. In Internet Explorer, the configuration must be set manually. In Mozilla Firefox, you can specify the SnapGear URL to the .pac file for automatic configuration.

To configure Internet Explorer for Web Cache

- 1 In Internet Explorer, click **Tools > Internet Options > Connections** tab > **LAN Settings**. The LAN Settings dialog box is displayed.

Figure 137: Web Cache - IE browser LAN settings

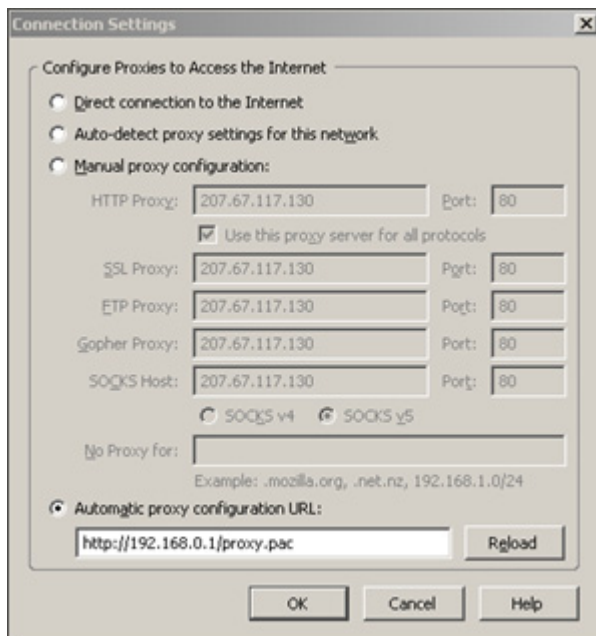


- 2 In the **Proxy Server** pane, set the fields as follows:
 - a Select the **Use proxy server...** check box.
 - b Enter the IP address of your SnapGear appliance in the **Address** box.
 - c Enter **3128** in the **Port** box. The Web cache of the SnapGear appliance uses port 3128 by default.
 - d Select the **Bypass proxy for local addresses** check box.
- 3 Click **OK**.

To configure Mozilla Firefox for Web Cache

- 1 In Firefox, click **Tools > Options > Connection Settings**. The Connection Settings dialog box is displayed.

Figure 138: Web Cache - Firefox Mozilla Connection Settings



- 2 Select the **Automatic proxy configuration URL** option.
- 3 Enter the location of the proxy .pac file:
`http://192.168.0.1/proxy.pac`
- 4 Click **OK**.

Allocating local USB storage for Web caching

Use this procedure to configure local USB storage for the Web cache.

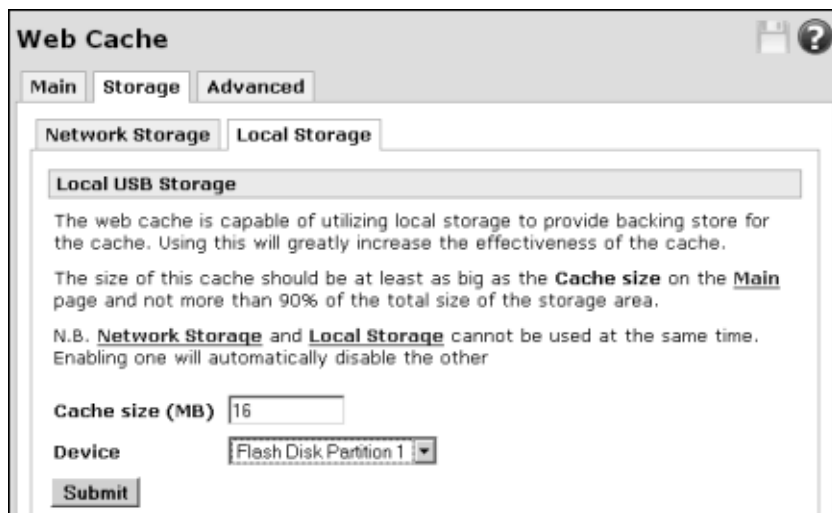
Note: Local USB storage is applicable to the SG565 model only.

If you prefer, you can use Network storage for the Web cache instead. See “Allocating network storage for Web cache” on page 180.

Prerequisite: Attach a USB storage device to a USB port.

- 1 From the **Network Setup** menu, click **Web Cache > Storage > Local Storage** tab. The Local USB Storage page appears.

Figure 139: Web Cache -
Local USB Storage



The screenshot shows the 'Web Cache' configuration window with the 'Storage' tab selected. Inside the 'Storage' tab, the 'Local Storage' sub-tab is active. The page contains the following elements:

- Local USB Storage** section header.
- Text: "The web cache is capable of utilizing local storage to provide backing store for the cache. Using this will greatly increase the effectiveness of the cache."
- Text: "The size of this cache should be at least as big as the **Cache size** on the **Main** page and not more than 90% of the total size of the storage area."
- Text: "N.B. **Network Storage** and **Local Storage** cannot be used at the same time. Enabling one will automatically disable the other"
- Cache size (MB)** field with a value of 16.
- Device** dropdown menu showing 'Flash Disk Partition 1'.
- Submit** button.

- 2 Enter the cache size in the **Cache Size** field. The size should be at least as big as the Cache size on the Main page (see “Web Cache — Main tab” on page 177) and not more than 90% of the total size of the share.
- 3 Select the partition or device to use from the **Device** list. For information on partitioning a USB device, see “Example: Partitioning a USB storage device” on page 529.
- 4 Click **Submit**.

Configuring Web Cache Peers

Use this procedure to configure a Web cache for peer parent and sibling caches. The Web cache boosts the performance of Web site access.

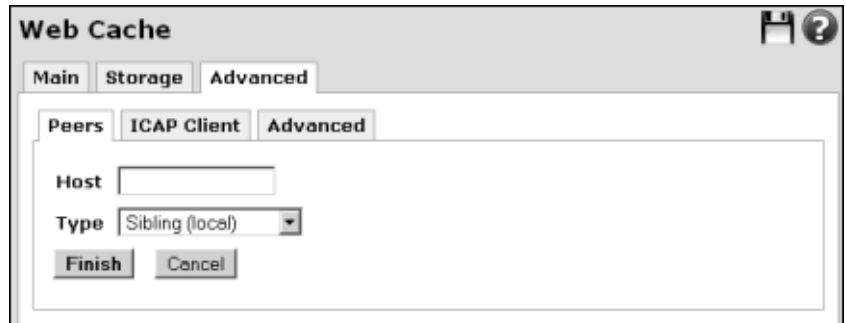
- 1 From the **Network Setup** menu, click **Web Cache > Advanced tab > Peers** tab. The Peers edit page appears.

Figure 140: Web Cache page edit Peers tab



- 2 Click **New**. The (new) Peers page appears.

Figure 141: Web Cache page new Peers tab



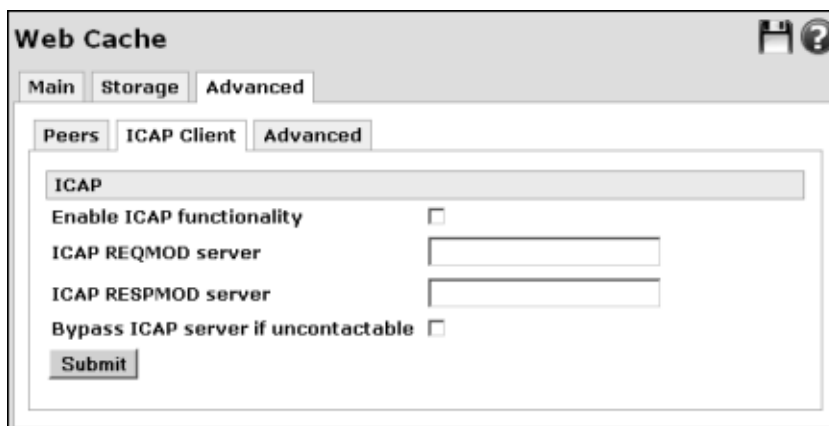
- 3 Enter the host or IP address of an ICP-capable Web cache peer in the **Host** field.
- 4 Select the relationship of the Host to the appliance's Web cache from the **Type** list. Available options are:
 - **Sibling (local):** If the peer is a sibling, then the appliance can only request Web objects already held in the peer's cache. The peer cannot forward cache misses on behalf of the device. These peers are not usually located in the direction of the appliance's route to the Internet.
 - **Parent (upstream):** If the peer is a parent, then the appliance forwards requests to the peer. If the peer does not have the requested Web object, it forwards the request on behalf of the appliance. These peers are usually located in the direction of the appliances's route to the Internet.
- 5 Click **Finish**. The peer is displayed in the edit list. For best results, configure both Sibling and a Parent Peers.

Configuring ICAP client for Web Cache

The ICAP client of the appliance allows you to use a third-party ICAP server as an intermediary between incoming traffic from the Web and LAN PCs browsing the Web. Outgoing Web requests or incoming Web traffic is passed off to the ICAP server for processing before being returned to the requesting LAN PC. The ICAP server can process outgoing Web requests from a LAN PC using a REQMOD service, or incoming Web traffic from an external Web server using a RESPMOD service. A typical function of a REQMOD service would be URL filtering. A typical function of a RESPMOD service would be virus scanning.

- 1 From the **Network Setup** menu, click **Web Cache > Advanced tab > ICAP Client** tab. The ICAP page appears.

Figure 142: Web Cache page ICAP Client tab

The screenshot shows the 'Web Cache' configuration interface. At the top, there are three tabs: 'Main', 'Storage', and 'Advanced'. The 'Advanced' tab is selected. Below this, there are three sub-tabs: 'Peers', 'ICAP Client', and 'Advanced'. The 'ICAP Client' sub-tab is selected. The main content area is titled 'ICAP' and contains the following options: 'Enable ICAP functionality' with an unchecked checkbox, 'ICAP REQMOD server' with an empty text input field, 'ICAP RESPMOD server' with an empty text input field, and 'Bypass ICAP server if uncontactable' with an unchecked checkbox. At the bottom of the form is a 'Submit' button.

- 2 Select the **Enable ICAP functionality** check box to enable the ICAP features of the Web cache.
- 3 Enter the URL for an ICAP server's REQMOD service in the **ICAP REQMOD server** field. The URL must begin with *icap://*. For example:
icap://192.168.0.10:1344/reqmod
- 4 Enter the URL for an ICAP server's RESPMOD service in the **ICAP RESPMOD server** field. The URL must begin with *icap://*. For example:
icap://192.168.0.10:1344/respmo
- 5 [Recommended] To bypass an unresponsive ICAP server, select the **Bypass ICAP server if uncontactable** check box. If the ICAP server is not responding to requests, Web transactions are allowed as normal. If this option is disabled, all Web transactions are blocked until the ICAP server becomes contactable.
- 6 Click **Submit**.

Configuring advanced settings for the Web cache

- 1 Under the **Network Setup** menu, click **Web Cache > Advanced** tab > **Advanced** subtab. The Advanced Configuration page appears.

Figure 143: Web Cache page Advanced tab

Web Cache

Main Storage **Advanced**

Peers ICAP Client **Advanced**

Advanced Configuration

Port

Extra diagnostic output ☐

Maximum cached object size (KB)

Maximum cached object size in memory (KB)

Transparent Proxy ☐

Interoperate with Access Controls ☐

The web cache is also capable of removing identifying information (to protect users' anonymity) from web requests that it services.

Anonymity Level

The web cache log files are usually stored in shared system memory. Do not increase these settings unless a Local Storage or Network Storage device is in use.

Log File Size (KB)

Log File Rotation Time (minutes)

Log File Rotations

Submit

- 2 In the **Port** field, specify the TCP network port the Web cache listens on, which is usually 3128 or 8080.
 - Default: 3128.
- 3 [Optional] To display extra information in addition to the usual cache log file in the system log, select the **Extra diagnostic output** check box.
- 4 Objects larger than the **Maximum cached object size (KB)** are not cached. To get a high bytes hit ratio, increase the cache size (one 32 MB object hit counts for 3200 10 KB hits). To increase speed at the expense of bandwidth, leave this setting low.
 - Default: 250
 - Integer value

- 5 Objects larger than the **Maximum cached object size in memory (KB)** are not kept in the memory cache. This should be set high enough to keep objects accessed frequently in memory to improve performance whilst low enough to keep larger objects from hoarding cache memory.
 - Default: 32
 - Integer value
- 6 [Optional] To enable the Web cache and access controls operate transparently, select the **Transparent proxy** check box. Transparent operation filters and caches Web traffic regardless of whether or not the clients on the LAN have specified an HTTP proxy in their Web browsers.
- 7 [Optional] To allow the Web cache to operate simultaneously with access controls, including content filtering and anti-virus, select the **Interoperate with Access Controls** check box.

Note: Due to limitations in peering proxies in this manner, user-based access controls will not work.

- 8 Select a level from the **Anonymity Level** list. The list controls the amount of identifying information removed from Web requests in order to protect your anonymity. The levels of protection are specified in increasing order and all but the first violate the HTTP standard and thus might cause problems with some Web sites. Available options are:
 - **None:** (default). No anonymity and no identifying information is removed from Web requests.
 - **Basic**
 - **Paranoid**
 - **Custom:** The Custom setting is for users who have manually edited these settings in the cache configuration file as it leaves the settings untouched.
- 9 Enter the maximum size of each log file before it gets rotated in the **Log File Size (KB)** field. If set to 0 (zero), the log files are rotated every time they are checked.
 - Default: 256
- 10 Specify how often the logs are checked for rotation in the **Log File Rotation Time (minutes)** field.
 - Default: 10

11 Specify how many log file rotations to store in the **Log File Rotations** field. The minimum default of 1 means 2 files are kept: the current log file and the previous log file. A maximum of 9 means 10 files are kept.

- Default: 1
- Range: 1-9

12 Click **Submit**.

QoS Traffic Shaping

The QoS (Quality of Service) traffic shaping is an advanced feature provided for expert users to fine-tune their network connections. Traffic shaping allows you to give preference to certain types of network traffic to maintain quality of service when a network connection is under heavy load.

Note: There must be only one LAN and one WAN in order to configure traffic shaping. At this time, traffic shaping is not supported for configurations that include multiple LANs and DMZs. For the SG565 model, the wireless connection must be unconfigured.

This section contains the following topics:

- "Enabling QoS Autosshaper"
- "Disabling QoS Autosshaper" on page 191
- "About ToS packet priority" on page 192
- "Enabling and configuring ToS packet priorities" on page 193
- "Creating a packet priority rule" on page 194
- "Editing a packet priority rule" on page 195
- "Deleting a packet priority rule" on page 195

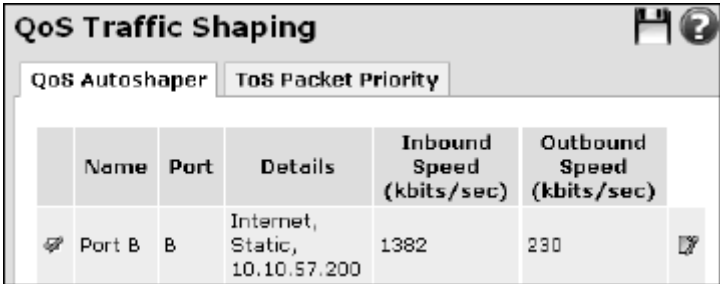
Enabling QoS Autosshaper

The Auto Traffic Shaper uses a set of built-in traffic shaping rules to attempt to ensure low latency on interactive connections, while maintaining fast throughput on bulk transfers.

Tip: To optimize traffic shaping performance, especially when using VoIP, set the outgoing interface MTU down to a value such as 500, overriding the default (typically 1400-1500). Go to the appropriate Connections subtab for the interface to edit the MTU setting. For more information, see "Connections" on page 35.

- 1 From the **Network Setup** menu, click **QoS Traffic Shaping**. The QoS Autosshaper page appears.

Figure 144: QoS Traffic Autosshaper



QoS Traffic Shaping					
QoS Autosshaper		ToS Packet Priority			
	Name	Port	Details	Inbound Speed (kbits/sec)	Outbound Speed (kbits/sec)
	Port B	B	Internet, Static, 10.10.57.200	1382	230

- 2 Click the edit icon next to the network interface on which you want to enable the autoshaper. Another QoS Autosshaper tab appears.

Figure 145: QoS Traffic Autosshaper

The screenshot shows a dialog box titled "QoS Traffic Shaping" with two tabs: "QoS Autosshaper" (selected) and "ToS Packet Priority". The "QoS Autosshaper" tab contains the following fields and controls:

- Port:** A dropdown menu showing "Port B".
- Enable:** A checked checkbox.
- Inbound Speed (kbits/sec):** A text input field containing "1382".
- Outbound Speed (kbits/sec):** A text input field containing "230".
- Buttons:** "Finish" and "Cancel" buttons at the bottom.

- 3 Select the **Enable** check box.
- 4 Enter the downstream speed of the network connection for the interface in kilobits per second in the **Inbound Speed** list.

Note: At least one entry for either inbound or outbound speed is required.

- 5 Enter the upstream speed of the network connection for the interface in kilobits per second in the **Outbound Speed** list.

Note: If you have a PPTP or PPPoE connection to the Internet, enter approximately 80–90% of the speed that the ISP supplied to account for protocol overheads. If you have a cable modem, DHCP, bridged, or other type of direct IP connection to the Internet, enter values from 90-100%.

The above example in Figure 145 assumes a speed of 1.5 MB down (inbound), 256 KB up (outbound). $1.5 \times 1024 = 1536$ kbits inbound. 90% of 1536 is 1382 kilobits. 90% of 256 is 230 kbits.

- 6 Click **Finish**.

Disabling QoS Autosshaper

- 1 From the **Network Setup** menu, click **QoS Traffic Shaping**. The QoS Autosshaper page appears.
- 2 Click the edit icon next to the network interface on which you want to disable the autosshaper. The QoS Autosshaper tab appears.
- 3 Clear the **Enable** check box.
- 4 Click **Finish**.

About ToS packet priority

Tos (Type of Service) packet prioritization feature provides a finer level of control over the relative performance of various types of IP traffic. You can allocate high, medium, or low priority to the following services:

- domain (tcp and udp)
- ftp and ftp-data
- http and https
- imap
- irc
- nntp
- ntp
- pop3
- smtp
- ssh
- telnet

Enabling and configuring ToS packet priorities

You can configure the ToS packet priorities for services. When the SnapGear appliance has multiple packets queued for transmission, it transmits the higher priority packets first. This priority is set in the ToS field in the IP packet header. The appliance is able to change the ToS field of some traffic types in order to increase their priority. Packets can also be matched by their source or destination IP address.

Tip: ToS traffic shaping works best when used in conjunction with the QoS autoshaper. Enable and configure the QoS autoshaper if possible when using ToS packet prioritization. See “Enabling QoS Autoshaper” on page 190.

When you enable ToS prioritization, the appliance sets up the following three bandwidth management queues:

- high priority queue with 55% guaranteed bandwidth and 100% maximum bandwidth.
- medium priority queue with 30% guaranteed bandwidth and 90% maximum bandwidth.
- low priority queue with 10% guaranteed bandwidth and 80% maximum bandwidth.

You can then specify which packets are to be classed as high, medium and low priorities. The packets are passed to the appropriate queue. Traffic that is not classified as high, medium, or low (that is, set to unchanged) is sent to the medium priority queue.

- 1 Under **Network Setup**, click **QoS Traffic Shaping > ToS Packet Priority** tab.

Figure 146: ToS Packet Priority

QoS Traffic Shaping

QoS Autoshaper **ToS Packet Priority**

Enable ToS Prioritization ☒

Default priority High

Submit

Services	Source Address	Destination Address	Priority
No entries			

New

- 2 Select the **Enable ToS Prioritization** check box.

- 3 Select a **Default priority** from the list. The Default priority is assigned to all network services other than those specifically defined in packet priority rules (see "Creating a packet priority rule"). Available options are:
 - **Unchanged**—Uses the ToS set by the sender. If a priority was not set by the sender, the packet is placed in the medium queue.
 - **Low**
 - **Medium**
 - **High**
- 4 Click **Submit**. An action successful message is displayed. ToS Packet Priority is now enabled and configured with a default priority. You can now assign priorities to specific services.

Creating a packet priority rule

- 1 Under **Network Setup**, click **QoS Traffic Shaping > ToS Packet Priority** tab. The ToS Packet Priority page appears.
- 2 Click **New**. The Add ToS Packet Priority rule page appears.

Figure 147: Add ToS Packet Priority rule

The screenshot shows the 'Add ToS Packet Priority rule' configuration window. It features a title bar with 'QoS Traffic Shaping' and icons for saving and help. Below the title bar are two tabs: 'QoS Autosshaper' and 'ToS Packet Priority'. The main area is titled 'Add ToS Packet Priority rule'. It contains four rows of configuration fields: 'Services' with a dropdown menu showing 'Any' and a 'New' button; 'Source Address' with a dropdown menu showing 'Any' and a 'New' button; 'Destination Address' with a dropdown menu showing 'Any' and a 'New' button; and 'Priority' with a dropdown menu showing 'Low'. At the bottom are 'Finish' and 'Cancel' buttons.







- 3 Select a service from the **Services** list. Or, to define a new service within this page, click **New**. The **Services** field changes to the **Protocol** and **Ports** fields.
- 4 [Conditional, if you are defining a new service within this page] Select a protocol for the service from the **Protocol** list. Available options are:
 - TCP
 - UDP
 - IP
 - ICMP

- 5 [Conditional, if you are defining a new service in this page] Enter a port, protocol, or ICMP message type in the **Ports** field. Acceptable inputs are:
 - service name
 - single port number between 1 and 65535
 - range of port numbers in the form *a-b*
 - comma- or whitespace-separated list of any of the above inputs

Tip: Click **Show Definitions** to select a definition already defined. For more information, see “Definitions” on page 219.

- 6 Select a source address from the **Source Address** list, or click **New** to enter a new IP address as a source.
- 7 Select a destination address from the **Source Address** list, or click **New** to enter a new IP address as a source.
- 8 Select a **Priority** from the list. Available options are:
 - **Low**
 - **Medium**
 - **High**
- 9 Click **Finish**. The rule is displayed in the Services list. You can edit and delete the definitions as needed.

Figure 148: Defined ToS Services

Services	Source Address	Destination Address	Priority		
POP3 (E-Mail)	My corp laptop	Any	High		
FTP	My corp laptop	Any	High		
NNTP (News)	Any	Any	Low		

Editing a packet priority rule

- 1 Under **Network Setup**, click **QoS Traffic Shaping > ToS Packet Priority** tab. The ToS Packet Priority page appears.
- 2 Click the edit icon for the rule you want to edit. An edit page appears for the rule.
- 3 Make your changes and click **Finish**.

Deleting a packet priority rule

- 1 Under **Network Setup**, click **QoS Traffic Shaping > ToS Packet Priority** tab. The ToS Packet Priority page appears.
- 2 Click the delete icon for the rule you want to delete. The rule is deleted from the service list.

IPv6 tab

Support for IPv6 is currently limited. The IPv6 page allows you to enable IPv6 routing for the appliance. When IPv6 routing is enabled, the following actions are performed:

- Site-local addresses are assigned to LAN connections.
- The site-local DNS server address (`fec0:0:0:ffff::1/64`) is assigned to LAN connections if the DNS proxy is enabled.
- Router advertisements are sent on LAN connections.
- 6to4 tunnels are created on Internet connections.
- A default set of IPv6 packet filter rules are enabled. These IPv6 packet filter rules are *stateless*, as opposed to the IPv4 packet filter rules, which are *stateful*. The default rules only support a single LAN connection and a single WAN connection. You can customize these rules on the Custom IPv6 Firewall Rules page. For further information, refer to “Custom IPv6 Firewall Rules tab” on page 244.

Enabling IPv6 at the appliance level

Use this procedure to enable IPv6 routing for the SnapGear appliance. You must also enable IPv6 for each connection that supports IPv6. For instructions, see “Enabling IPv6 for a connection” on page 44.

- 1 From the **Network Setup** menu, click **Network Setup > IPv6** tab. The IPv6 page appears.

Figure 149: IPv6 page

- 2 To enable IPv6 routing and packet filtering, select the **Enable IPv6** check box.
- 3 Click **Submit**.

Disabling IPv6

Use this procedure to disable IPv6 at the appliance level. Disabling at the appliance level disables IPv6 for connections as well even though they are still enabled at the connection level.

- 1 From the **Network Setup** menu, click **Network Setup > IPv6** tab. The IPv6 page appears.
- 2 Clear the **Enable IPv6** check box.
- 3 Click **Submit**.

SIP Proxy tab

Note: SIP is applicable to SnapGear Models SG565, SG580, and SG720 only.

SIP (Session Initiation Protocol, RFC3261) is the protocol of choice for most VoIP phones to initiate communication. By itself, SIP does not work from behind masquerading firewalls, as the transferred data contains IP addresses and port numbers.

The SIP proxy of the SnapGear appliance allows SIP software clients or SIP hardware clients to work from a private network (such as your LAN) behind a masquerading firewall such as the one on the SnapGear appliance. SIP software includes clients like kphone, linphone, and SJphone. SIP hardware includes VoIP (Voice over IP) phones that are SIP-compatible, such as those from Cisco, Grandstream, and Snom.

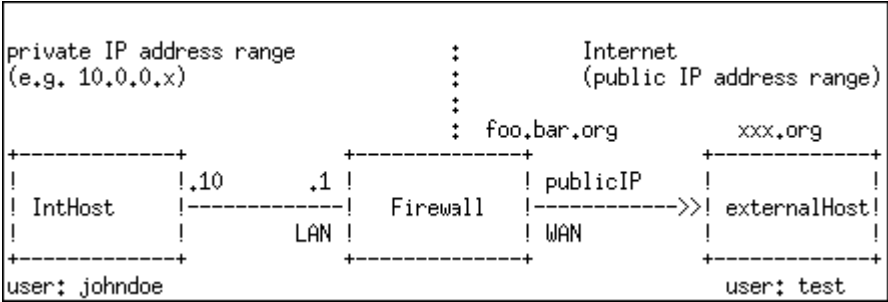
If you use an external SIP service such as the Gizmo Project or Skype, you typically do not need to use the SIP proxy. These services use STUN (Simple Traversal of UDP through NATs) to facilitate communication from behind a masquerading firewall.

The SIP proxy listens on UDP port 5060 for SIP requests. This is the standard SIP port and should not generally need to be changed. The SIP proxy listens on UDP ports 7070-7079 for RTP traffic, which is the actual voice data.

The SIP proxy allows seamless communication between SIP phones running on an internal network (LAN or DMZ) and SIP phones in the wider Internet. See the Siproxd Web site for full details: <http://siproxd.sourceforge.net/>

A typical SIP configuration is shown in Figure 150:

Figure 150: Example SIP proxy configuration

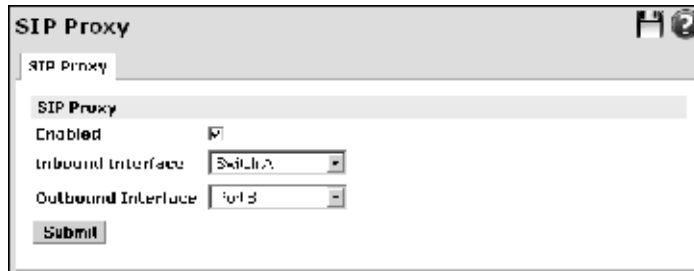


- The internal host is running a SIP softphone (like linphone, kphone)
- The SIP address used by the internal host is *sip:johndoe@foo.bar.org*
- The softphone on the internal host is configured to register at the SIP proxy running on the firewall as *sip:johndoe@foo.bar.org*
- *foo.bar.org* is the domain name corresponding to the public IP address of the firewall
- The external host does not register with the firewall

Enabling the SIP proxy

- 1 From the **Network Setup** menu, click **SIP**. The SIP Proxy page appears.

Figure 151: SIP Proxy page



The screenshot shows the 'SIP Proxy' configuration window. It has a title bar with the text 'SIP Proxy' and a help icon. Below the title bar is a tabbed interface with a single tab labeled 'SIP Proxy'. The main content area contains the following elements: a section header 'SIP Proxy', an 'Enabled' checkbox which is checked, an 'Inbound Interface' dropdown menu currently showing 'eth0', an 'Outbound Interface' dropdown menu currently showing 'eth1', and a 'Submit' button at the bottom.

- 2 [Optional] Select the **Enabled** check box.
- 3 Select an interface from the **Inbound Interface** list. The inbound interface is typically the **Internet** interface. The inbound interface is the interface through which remote SIP clients can be reached.
- 4 Select an interface from the **Outbound Interface** list. The outbound interface is typically the **LAN** interface. This is the interface connected to your private network on which SIP clients are located.
- 5 Click **Submit**.

Details of incoming and outgoing calls are logged in the system log. To view the log, from the **System** menu, click **Diagnostics** > **System Log** tab.

Disabling the SIP proxy

- 1 From the **Network Setup** menu, click **SIP**. The SIP Proxy page appears.
- 2 Clear the **Enabled** check box.

CHAPTER 3

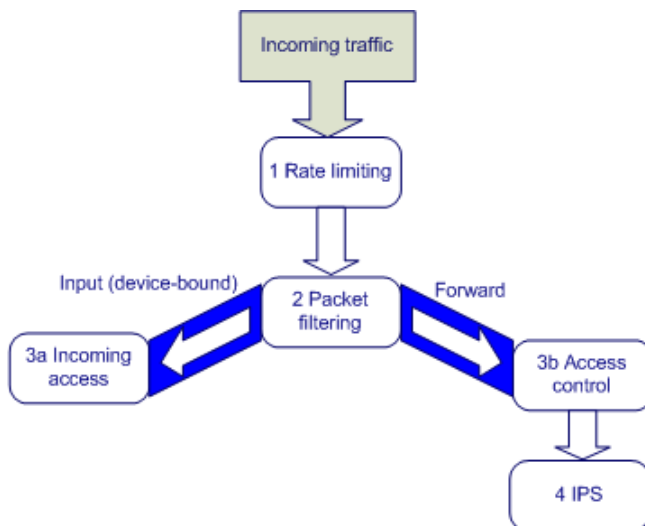
Firewall menu

Controlling packet traffic	202
Incoming access.....	204
Definitions.....	219
Packet filtering.....	231
NAT	245
Connection tracking.....	274
Intrusion Detection Systems.....	284
Access control	297
Antivirus.....	327
Antispam (TrustedSource).....	340

Controlling packet traffic

Many features within the SnapGear management console can affect the flow of packet traffic within the appliance. This topic outlines the hierarchy and precedence of the features. The vast majority of incoming traffic are forwarded packets. Packets considered as Input (device-bound) are destined for the SnapGear appliance itself, targeted as either a device endpoint, Web-administration, proxy, or sshd.

Figure 152: Control flow hierarchy



- 1 Rate limiting:** All packets are subject to packet flood rate limiting if it is enabled in Connection tracking. For details, see “Configuring connection tracking” on page 276.
- 2 Packet filtering:** Traffic is then subjected to packet filtering. See “Packet filtering” on page 231. Also, if rate limiting on a rule is enabled, a second rate limiting is applied. See “Rate limiting a packet filter rule” on page 237.
- 3** After packet filtering rules are applied, packets are directed either to Incoming Access or Access Control:
 - a Incoming Access:** Packets destined for the appliance (Inputs) are processed by Incoming Access rules. See “Incoming access” on page 204.
 - b Access Control:** All other packets travelling through the appliance (Forwards) that are not blocked by packet filtering are turned over to access control. For details, see “Access control” on page 297.
- 4 IPS:** If IPS is enabled, packets pass to IPS after handling by Access Control mechanisms. For details, see “Intrusion Detection Systems” on page 284.

Firewall overview

The SnapGear appliance is equipped with a fully-featured firewall. The firewall allows you to control both incoming and outgoing access so that PCs on local networks can have tailored Internet access facilities while being shielded from malicious attacks from external networks. The stateful firewall of the appliance keeps track of outgoing connections, such as a PC on your LAN requesting content from a server on the Internet, and only allows corresponding incoming traffic, such as the server on the Internet sending the requested content to the PC. By default, your appliance allows network traffic as shown in Table 13:

Table 13: Default network traffic

Incoming Interface	Outgoing Interface	Action
LAN	Any	Accept
VPN	Any	Accept
Dial-in	Any	Accept
DMZ	Internet	Accept
DMZ	Any except Internet	Drop
Internet	Any	Drop
Guest	Any	Drop

Sometimes it is useful to allow some incoming connections; for example, if you have a mail or Web server on your LAN or DMZ that you want to be accessible from the Internet. This is accomplished using a combination of NAT and packet filter rules. The Web management console provides a powerful interface for tailoring the firewall to your network.

The Firewall menu contains the following topics for its menu options (some models do not have all menu options):

- “Incoming access” on page 204
- “Definitions” on page 219
- “Packet filtering” on page 231
- “NAT” on page 245
- “Connection tracking” on page 274
- “Intrusion Detection Systems” on page 284
- “Access control” on page 297
- “Antivirus” on page 327
- “Antispam (TrustedSource)” on page 340

Incoming access

The Incoming Access menu option allows you to control access to the SnapGear appliance itself, such as for remote administration. The following pages are available from the Incoming Access menu option:

- Administration Services page
- Web Management Configuration page

Administration Services page

By default, the SnapGear appliance runs a Web administration server, a Telnet, and an SSH service (SSH is not applicable to the SG300 model). Access to these services can be restricted to specific interfaces. Typically, access to the Web management console (Web/SSL Web) is restricted to hosts on your local network (LAN Interfaces).



Security Alert: If you want to allow administrative access on interfaces other than LAN Interfaces, there are additional security precautions you should take, such as setting up packet filter rules. For further information, see “Packet Filter Rules page” on page 232. Also consider remote administration using a VPN connection as an alternative to opening a hole in the firewall; PPTP in particular is well-suited to this task. PPTP is also an alternative to packet filter rules if you are not connecting from a static IP address, which is required for packet filters to function. For more information, see “About VPN” on page 348.

Figure 153 shows the Administration Services page for the SG565 model:

Figure 153:
Administration Services
page-SG565 model

Administration Services

Administration Services

Web Management

Administration Services

By default the SnapGear unit runs a web administration service and a telnet service. You can enable these services on specific interface types by checking the boxes below.

Warning: Disabling **all** of the services will make future configuration changes to the unit impossible without a factory reset.

	Telnet	SSH	Web (HTTP)	SSL Web (HTTPS)
LAN interfaces	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Internet interfaces	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DMZ interfaces	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Guest interfaces	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Dial-in interfaces	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

ICMP messages relating to existing connections are always accepted. You can also choose to accept ICMP echo request messages on Internet interfaces.

Accept echo request (incoming ping) ☒

Submit

The interfaces and services that appear in this page depend on the particular SnapGear appliance. Table 14 provides information about the services you can enable for each interface:

Table 14: Interface service descriptions

Service	Description
Telnet	This column controls access to the SnapGear appliance via a telnet command line interface. Only Administrative users with the Login access control enabled are able to connect via telnet. See “Creating an administrative user” on page 476. Administrative users connected via the telnet interfaces have complete access to the configuration of the appliance. Telnet is completely unencrypted. Disabling Telnet services is recommended for increased security.
SSH	This column controls access to the SnapGear appliance via a Secure Shell (SSH) command line interface. Only Administrative users with the Login access control enabled are able to connect via telnet. See “Creating an administrative user” on page 476. SSH provides for secure encrypted communication whereas telnet is completely unencrypted. Administrative users connected via the SSH interface have complete access to the configuration of the appliance. <i>Note: SSH is not currently available on the SG300 model.</i>
Web (HTTP)	This column controls access to the SnapGear appliance via the SnapGear Web management console. To use the console, ensure that the SnapGear appliance's Web server is configured appropriately in the Web Management page. See “Configuring the Web management console” on page 208.
SSL Web (HTTPS)	This column controls access to the SnapGear appliance via the SnapGear Web management console. To use the console, ensure that the SnapGear appliance's Web server is configured appropriately in the Web Management page. See “Creating an administrative user” on page 476.

Accepting incoming echo requests

The Accept echo request check box governs how ICMP requests are processed for Internet, DMZ, and Guest interfaces. Selecting this check box enables ICMP requests on all of the interfaces that use the Internet, DMZ, or Guest firewall class. To selectively enable ICMP requests, the Accept echo request check box must be cleared and an appropriate Input-Accept packet filter rule generated.

If accept echo request is enabled, the corresponding Accept action is processed prior to GUI-configured packet filter rules, and as such, adding packet filter rules will not have any effect. That is, you cannot selectively drop ICMP requests with a default of accept; you can only selectively accept ICMP requests with a default of drop.

There are some advantages to using specific packet filter rules for ICMP requests rather than this check box, as packet filter rules have configurable rate limits, and can also be used to limit the specific source-addresses from which ICMP requests are allowed. For more information on packet filter rules, see “Packet filtering” on page 231.

Configuring administrative services access

- 1 From the **Firewall** menu, click **Incoming Access**. The Administration Services page appears.

Figure 154:
Administration Services
page — SG300 model

Administration Services

Administration Services

Web Management

Administration Services

By default the SnapGear unit runs a web administration service and a telnet service. You can enable these services on specific interface types by checking the boxes below.

Warning: Disabling **all** of the services will make future configuration changes to the unit impossible without a factory reset.

	Telnet	Web (HTTP)	SSL Web (HTTPS)
LAN interfaces	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Internet interfaces	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Dial-in interfaces	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

ICMP messages relating to existing connections are always accepted. You can also choose to accept ICMP echo request messages on Internet interfaces.

Accept echo request (incoming ping) ☐

Submit

- 2 Select or clear the check boxes for the services you want to enable or disable.



Caution: *Disallowing all services is not recommended, as this makes future configuration changes impossible unless your appliance is reset to the factory default settings.*

- 3 To allow echo requests on Internet interfaces, select the **Accept echo request (incoming port)** check box. The default (recommended) is to disallow echo requests, so your SnapGear appliance does not respond to pings on its own Internet interfaces. Disallowing echo requests may make it more difficult for external attackers scanning for hosts to discover your appliance. Destination unreachable ICMP messages are always accepted.
- 4 Click **Submit**.

Web Management Configuration page

You can enable or disable HTTP protocols, change HTTP port numbers, and create or upload certificates for securing access to the Web Management Console via HTTPS on the Web Management page.

Ideally, you should use packet filter rules to restrict access for remote administration. For information, see “Packet Filter Rules page” on page 232. Using packet filter rules, you can configure the appliance so that only connections originating from trusted IP addresses are allowed access to the administrative Web server port.

Configuring the Web management console

Use this procedure to configure access to the Web management console.



Caution: Do not disable both HTTP and HTTPS access to the Management Console or you will not be able to access the Web management console at all. If this occurs, edit the configuration file using SSH to reestablish access. Instructions for re-enabling Web interface access are available in the SnapGear Knowledgebase, article #3457.

- 1 From the **Firewall** menu, click **Incoming Access > Web Management** tab. The Web Management Configuration page appears.

Figure 155: Web Management Configuration

Web Management Configuration

Administration Services **Web Management**

Web Management Configuration

The SnapGear unit can be configured to run its web admin server on a port other than the HTTP default (80). Changing the default administration port is recommended if you intend to allow the unit to be configured externally, not just from the trusted (LAN) side on your network.

Note: To continue SnapGear configuration you will need to point your browser to the unit's new administration port (e.g. a device at IP address 10.0.0.1 using administration port 888 is <http://10.0.0.1:888/>)

Enable HTTP Management ☒

Port for HTTP

Enable HTTPS Management ☒

Port for HTTPS

Authenticate Default Page ☐

Submit **Upload Certificate** **Create Certificate**

- 2 Ensure the **Enable HTTP Management** check box is selected.
 - Default: Enabled

- 3 The Web management console runs on the default HTTP port 80. To use the default port for another purpose, change the port number in **Port for HTTP** field.

- Default: 80
- Range: Integer value between 1-65535

If you change the Web server port number, you must include the new port number in the URL to access the pages. For example, if you change the Web administration to port number 888, the URL to access the Web administration is similar to: <http://192.168.0.1:888>.

- 4 [Optional, recommended] To enable secure HTTP (HTTPS), select the **Enable HTTPS Management** check box.
- 5 [Optional] The Web management console runs on the default HTTPS port 443. You can change the port number in the **Port for HTTPS** field.
 - Default: 443
 - Range: Integer value between 1-65535

To access the Web management console securely using SSL encryption, add an “s” to http so that the URL becomes **https://** instead of **http://**. An example URL: <https://10.0.0.1:443>

If you plan to use secure HTTP to access the console, either uploading an SSL certificate or manually creating a more customized certificate than the default out-of-box certificate is recommended. For instructions, see “Uploading an SSL certificate” on page 210 and “Creating an SSL certificate” on page 211.

- 6 [Optional, recommended] To enable authentication for the default Web page of the SnapGear Management Console, select the **Authenticate Default Page** check box as an extra security precaution. It is recommended you enable this setting if you have enabled access for Internet interfaces on the Administration Services page. For more information, see “Administration Services page” on page 204.
 - Default: Disabled
- 7 Click **Submit**.

Certificates for HTTPS

As of version 3.1.4 of the firmware, a certificate for HTTPS (Secure HTTP) access is generated automatically when the appliance is first booted. The certificate contains default information for country, city, and related fields. It is enough to allow HTTPS access out-of-the-box, and it is relatively secure as no two SnapGear appliances have the same certificate. However, it is strongly recommended that an appropriate site-specific certificate either be uploaded or manually created at the earliest possible convenience. A proper certificate enables remote clients to establish its authenticity upon connection using chain of trust, root-cert signed, or site-specific fingerprint. If you have purchased or created SSL certificates for a Web server, you can upload them to the appliance.

Uploading an SSL certificate

- 1 From the **Firewall** menu, click **Incoming Access > Web Management** tab. The Web Management configuration page appears.
- 2 Click **Upload certificate**. The Upload Certificate page appears.

Figure 156: Upload Certificate

- 3 Click **Browse** to locate the **Local Certificate** (RSA x509 certificate) and its corresponding **Private Key Certificate**.
- 4 Click **Submit**.

Creating an SSL certificate

Use this procedure to manually create or update a self-signed certificate on the SnapGear appliance. The optional fields are used to create the distinguished name of the certificate. For best results, complete all optional fields.

When you access the Web management console using HTTPS, your Web browser may give warnings about the authenticity of the certificate since it has not been signed by a known Certificate Authority. For more information, see “Uploading an SSL certificate” on page 210. Otherwise, if you want to import your certificate into the IE browser, see “Installing your certificate in your browser” on page 213.

To create a certificate

- 1 From the **Firewall** menu, click **Incoming Access > Web Management** tab. The Web Management Configuration page appears.
- 2 Click **Create SSL certificates**. The SSL Certificate Setup page appears.

Figure 157: SSL Certificate Setup

The screenshot shows the 'SSL Certificate Setup' page within the 'Web Management' tab. The form contains the following fields and controls:

- Country:** A dropdown menu currently set to 'United States'.
- State or Province:** An empty text input field.
- Locality or City:** An empty text input field.
- Organization or Company:** An empty text input field.
- Section or Organizational Unit:** An empty text input field.
- Host name (Common Name):** A text input field containing the IP address '172.16.1.1'.
- Email Address:** An empty text input field.
- Generate an RSA key of:** A dropdown menu set to '2048 bits'.
- Buttons:** 'Submit' and 'Cancel' buttons at the bottom left.

- 3 [Optional] Select the appropriate country from the **Country** list.
- 4 [Optional] Enter the state or province in the **State or Province** field.
- 5 [Optional] Enter the name of your organization in the **Organization or Company** field.
- 6 [Optional] Enter your department in the **Section or Organization appliance** field.
- 7 Enter the IP address in the **Host name** field.
- 8 [Optional] Enter an email address in the **Email Address** field.

- 9 Select a certificate key length from the **Generate an RSA key of list**.

Available options are:

- **512 bits (default)**
- **1024 bits**
- **1536 bits**
- **2048 bits**
- **3072 bits**
- **4096 bits**

Note: *The more bits in the key, the longer it takes to generate the certificate. Larger keys take much longer to generate than smaller keys. A 1024-bit key takes more than double the amount of time to generate than a 512-bit key. Similarly a 4096-bit key takes more than four times as long as it would take for a 1024-bit key. Patience is advised when generating 4096-bit keys. Key generation is a very CPU-intensive operation that is not directly related to the effort required to use the key.*

- 10 Click **Submit**. A message informs you that an SSL certificate is currently being created. Generating a certificate usually takes a few minutes; exact time depends on the model of SnapGear appliance and the key length. When the certificate has been created, the message “A valid SSL certificate has been installed” is displayed under the Web Management tab.

Installing your certificate in your browser

Use this procedure to install your manually created certificate into the Internet Explorer browser. The certificate is already installed on the SnapGear appliance.

Prerequisites:

- Create a self-signed certificate manually with more detail than the shipped default. See “Creating an SSL certificate” on page 211.
- Enable HTTPS. See “Web Management Configuration page” on page 208.

When you access the Web management console using HTTPS, your Web browser may give warnings about the authenticity of the certificate since it has not been signed by a known Certificate Authority. This procedure installs the certificate in the browser to eliminate the Security Alert shown in Figure 158.



Security Alert: *The warning given by your browser about the risks of installing a root-CA are well-warranted. It is very important that you take care to protect your private root certificate. Should an untrusted party access your root-CA, it would enable that party to generate SSL certs that your browser would silently accept, thus compromising your security. Do not leave unencrypted backups of your SG configuration in unprotected places and be wary of granting access to your SG appliance. Such risks are much reduced when using a commercial root-CA.*

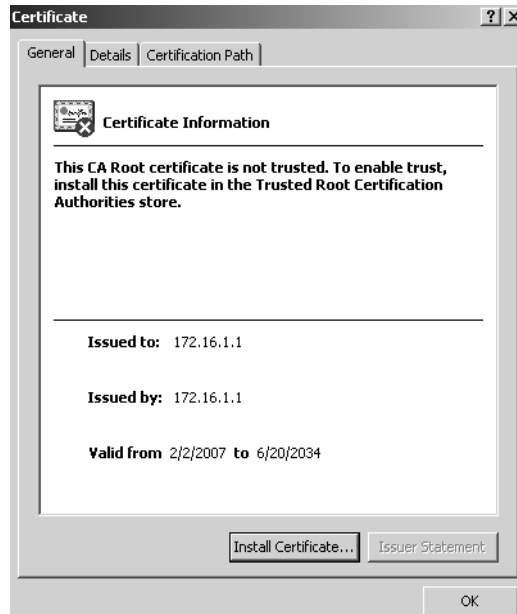
Uploading a certificate signed by an authority is the most secure and recommend method, however. For more information, see “Uploading an SSL certificate” on page 210.

Figure 158: Certificate warnings



- 1 Access the SnapGear Web management console via your HTTPS URL.
- 2 When the IE browser's Security Alert dialog box is displayed, click **View Certificate**. The general certificate information is displayed.

Figure 159: General Certificate Information



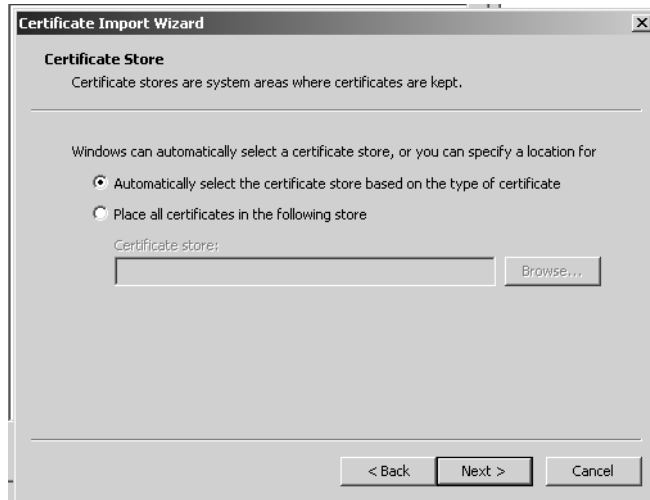
- 3 You can view the Details or Certification by click the relevant tab. Click **Install Certificate**. The wizard begins.

Figure 160: Certificate Import Wizard 1



- 4 Click **Next**. The Certificate Store page appears.

Figure 161: Certificate Import Wizard - Certificate Store



- 5** Select the **Automatically select store based on type** option and click **Next**.

Figure 162: Certificate Import Wizard - Certificate Store



- 6** Click **Finish**.

Figure 163: Certificate Import Wizard - Completing page



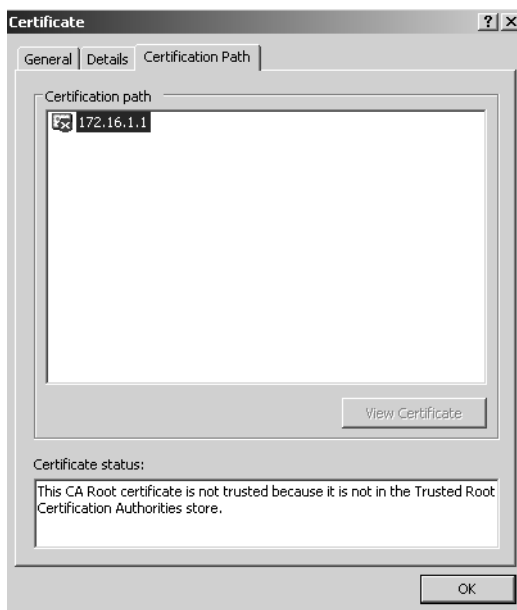
- 7 A security warning dialog box displays the thumbprint and requests you to confirm the import.

Figure 164: Security Warning - Thumbprint



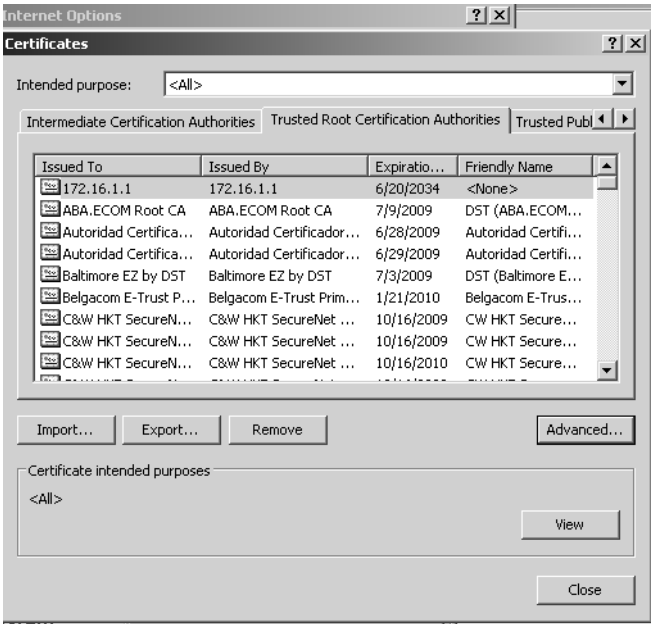
- 8 Click **Yes**. The Certification Path is displayed.

Figure 165: Certificate Certification Path



- 9 Click **OK**. You will no longer receive alerts when you access the console via https.
- 10 To view the certificates installed in the browser, click **Tools > Internet options > Content** tab > **Certificates** button. The Certificates dialog box appears.

Figure 166: IE browser installed certificates



Definitions

The SnapGear console provides definitions to assist with customizing your security policy. Definitions are used in packet filter or NAT rules, which allows for granularity in the rules and subsequently, a more manageable security policy.

Definitions are objects created to define the service group, address, and interface entities:

- **Service Group** — A definition that consists of a single service or a set of services.
- **Address** — A definition that defines a single IP address or a range of addresses.
- **DNS Hostname** — A definition that defines a DNS hostname.
- **Address Group** — A definition that consists of a set of definitions. Groups can consist of Address, DNS Hostname, and Address Group definitions.
- **Interface Group** — A definition that consists of a set of SnapGear interfaces.

Before creating packet filter or NAT rules, it is sometimes useful to define services or groups of services, addresses, and interfaces used to match packets. Definitions need not be created for simple rules that only specify a single service, address, or interface, as these can be entered while creating the rule. If a rule specifies groups of services, addresses, or interfaces, then you must create definitions for these groups before you create the rule.

The Definitions menu contains the following pages:

- "Service Groups page"
- "Addresses page"
- "Interfaces page"

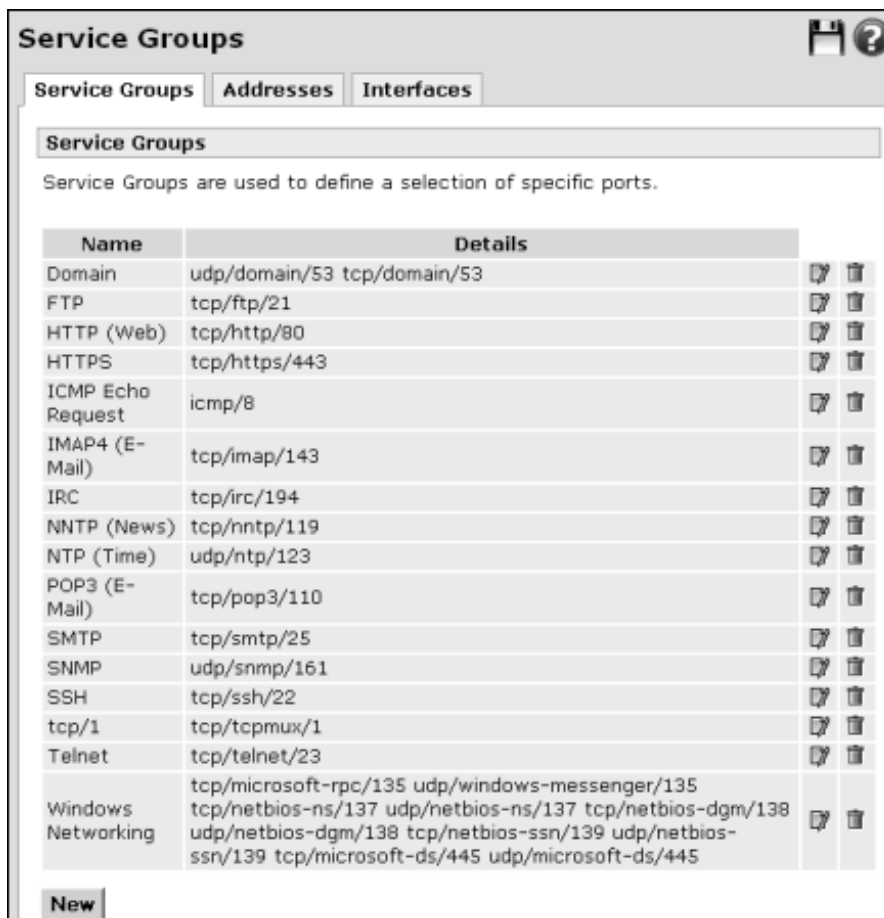
Service Groups page

A *service group* can be used to group together similar services. For example, you can create a group of services that you want to allow, and then use a single rule to allow them all at once. A service can belong to multiple service groups. You can refer to a service group in multiple packet filter rules. If you then modify the service group, all of the packet filter rules then use the modified service group.

A network service is defined by a protocol and port. Protocol can be either TCP, UDP, ICMP or IP. The port can be any valid network port number between 1 and 65535. As an example, HTTP (Web) uses the TCP protocol, with a default port of 80. Network packets may be matched by destination service.

The Service Groups page is shown in Figure 167:

Figure 167: Service Groups tab



Creating a service group

- 1 From the **Firewall** menu, click **Definitions > Service Groups** tab. The Service Groups page appears.

Predefined services are displayed. The **Name** column displays the name of the service group, and the **Details** column displays the protocol and port number. You can click the edit or delete icon to edit or delete the existing service groups.

- 2 Click **New**.

The Modify Service Group page appears.

Figure 168: Modify Service Group page

Service Groups

Service Groups | Addresses | Interfaces

Modify Service Group

Name

Domain (UDP) ☐

Domain (TCP) ☐

FTP ☐

HTTP (Web) ☐

HTTPS ☐

IMAP4 (E-Mail) ☐

IRC ☐

NNTP (News) ☐

NTP (Time) ☐

POP3 (E-Mail) ☐

SMTP ☐

SNMP ☐

SSH ☐

Telnet ☐

ICMP Echo Request (Ping) ☐

Other TCP Ports

Other UDP Ports

IP Protocols

ICMP Types

Finish Cancel

- 3 Enter a name for the service group in the **Name** field.
- 4 Select the services for the group from the list of predefined services.
- 5 To define a custom TCP, UDP, IP, or ICMP service, enter the appropriate port number. You can enter multiple numbers. Separate each entry with a comma.
- 6 Click **Finish**.

Editing a service group

- 1 From the **Firewall** menu, click **Definitions > Service Groups** tab. The Service Groups page appears.
- 2 Click the edit icon for the service group you want to edit. The Modify Service Group page appears.
- 3 Make your changes and click **Finish**.

Deleting a service group

- 1 From the **Firewall** menu, click **Definitions > Service Groups** tab. The Service Groups page appears.
- 2 Click the delete icon for the service group you want to delete.

Example: Creating a service group

This example create a service group named “Internet-services” that consists of the following services: HTTP, HTTPS, FTP, Ping, and SSH.

- 1 From the **Firewall** menu, click **Definitions > Service Groups** tab. The Service Groups page appears.
- 2 Click **New**. The Modify Service Group page appears.
- 3 Enter **Internet-services** in the **Name** field.
- 4 Select the following check boxes:
 - **FTP**
 - **HTTP (Web)**
 - **HTTPS**
 - **SSH**
 - **ICMP Echo Request (Ping)**
- 5 Click **Finish**.

Addresses page

Addresses are a single IP address, or range of IP addresses, or a DNS hostname. Network packets can be matched by source or destination address. There is no need to add addresses for the interfaces of the SnapGear appliance; these are predefined. The Addresses page is shown in Figure 169:

Figure 169: Addresses tab

Addresses

Service Groups | **Addresses** | Interfaces

Addresses

Define names for specific IP addresses or networks.

Name	Type	Details		
RFC1918 A	Single Address or Range	10.0.0.0/8		
RFC1918 B	Single Address or Range	172.16.0.0/12		
RFC1918 C	Single Address or Range	192.168.0.0/16		
RFC1918	Address Group	RFC1918 A, RFC1918 B, RFC1918 C		

New Single Address or Range

Adding an IP address or range

- 1 From the **Firewall** menu, click **Definitions > Addresses** tab. The Addresses page opens. Predefined addresses are displayed.
- 2 Select **Single Address or Range** from the **Type** list.
- 3 Click **New**. The Address Range page appears.

Figure 170: Address Range page

Addresses

Service Groups | **Addresses** | Interfaces

Address Range

Name

IP Address

Finish **Cancel**

- 4 Enter the name of the range in the **Name** field.
- 5 Enter the IP address or range in the **IP Address** field.
- 6 Click **Finish**.

Example: Adding a single IP address

This example adds a single IP address for the administration personal computer used to manage the appliance.

- 1 From the **Firewall** menu, click **Definitions > Addresses** tab. The Addresses page opens. Predefined addresses are displayed.
- 2 Select **Single Address or Range** from the **Type** list.
- 3 Click **New**. The Address Range page appears.
- 4 Enter **Admin-PC** in the **Name** field.
- 5 Enter **192.168.0.1** in the **IP Address** field. If your administrative PC for the appliance has a different IP address, use that in place of the default given for this example.
- 6 Click **Finish**.

Creating a DNS Hostname



Caution: DNS hostnames are not generally recommended for enforcing security policies. They are unreliable and can cause significant delays in updating the firewall rules.

- 1 From the **Firewall** menu, click **Definitions > Addresses** tab. The Addresses page appears.
- 2 Select **DNS Hostname** from the **Type** list.
- 3 Click **New**. The Hostname page appears.

Figure 171: Hostname page

The screenshot shows the 'Addresses' configuration window. At the top, there are three tabs: 'Service Groups', 'Addresses' (which is selected), and 'Interfaces'. Below the tabs, the 'Hostname' section is visible, containing a text input field labeled 'Hostname'. At the bottom of the window, there are two buttons: 'Finish' and 'Cancel'.

- 4 Enter a fully-qualified host name in the **Hostname** field.
- 5 Click **Finish**.

Example: Adding a DNS hostname

- 1 From the **Firewall** menu, click **Definitions > Addresses** tab. The Addresses page appears.
- 2 Select **DNS Hostname** from the **Type** list.
- 3 Click **New**. The Hostname page appears.
- 4 Enter **www.myhostname.com** in the **Hostname** field, where *myhostname* is the host you want to designate.
- 5 Click **Finish**.

Creating an Address Group

Group previously added addresses together to simplify your firewall ruleset.

- 1 From the **Firewall** menu, click **Definitions > Addresses** tab. The Addresses page appears.
- 2 Select **Address Group** from the **Type** list.
- 3 Click **New**. The Address Group page appears.

Figure 172: Address Group page

	Name	Type	Details
<input type="checkbox"/>	RFC1918 A	Single Address or Range	10.0.0.0/8
<input type="checkbox"/>	RFC1918 B	Single Address or Range	172.16.0.0/12
<input type="checkbox"/>	RFC1918 C	Single Address or Range	192.168.0.0/16
<input type="checkbox"/>	Port B	Network Interface	Internet, Static, 10.10.57.200
<input type="checkbox"/>	Switch A	Network Interface	LAN, Static, 192.168.0.1
<input type="checkbox"/>	WIFI (Wireless)	Network Interface	LAN, Static, 172.16.1.1
<input type="checkbox"/>	RFC1918	Address Group	RFC1918 A, RFC1918 B, RFC1918 C

- 4 Enter a descriptive name for the address group in the **Name** field.
- 5 Select the check boxes for the addresses, interfaces, or address groups you want to group together.
- 6 Click **Finish**.

Editing an IP address, address group, or DNS hostname

- 1 From the **Firewall** menu, click **Definitions > Addresses** tab. Addresses that have already been defined are displayed.
- 2 Click the edit icon for an existing address, address group, or DNS Hostname you want to edit. The edit page appears.
- 3 Make your changes and click **Finish**.

Deleting an address

Use this procedure to delete a single IP address, range of addresses, or address group. If an address is being used by a packet filter or NAT rule, a message informs you to modify or delete the rule that references the address. After you remove the reference to the address within the rule, you can delete the address.

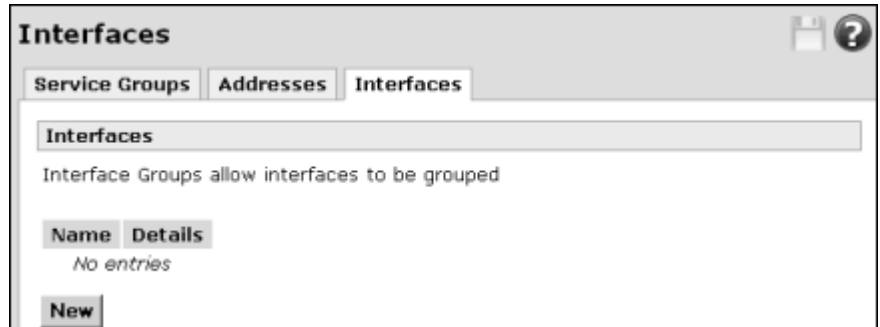
- 1 From the **Firewall** menu, click **Definitions > Addresses** tab. Addresses that have already been defined are displayed.
- 2 Click the delete icon for the object you want to delete.

Interfaces page

Use the Interfaces page to define, edit, and delete interface groups. Packets can also be matched by incoming and outgoing Interface. You can group the appliance network interfaces into Interface Groups to simplify your firewall ruleset.

The Interfaces page is shown in Figure 173:

Figure 173: Interfaces page



Defining an Interface Group

Use this procedure to define an interface group.

- 1 From the **Firewall** menu, click **Definitions > Interfaces** tab. The Interfaces page appears.
- 2 Click **New**. The Interface Group page appears.

Figure 174: Interface Group page

Interfaces

Service Groups | Addresses | **Interfaces**

Interface Group

Name

	Name	Details
<input type="checkbox"/>	Any Dial-In interface	
<input type="checkbox"/>	Any DMZ interface	
<input type="checkbox"/>	Any Guest interface	
<input type="checkbox"/>	Any Internet interface	
<input type="checkbox"/>	Any LAN interface	
<input type="checkbox"/>	Any VPN interface	
<input type="checkbox"/>	Switch A	LAN, Static, 192.168.0.1
<input type="checkbox"/>	Port B	Internet, Static, 10.10.57.200
<input type="checkbox"/>	WIFI (Wireless)	LAN, Static, 172.16.1.1

Finish **Cancel**

- 3 Enter a descriptive name in the **Name** field.
- 4 Select the check boxes for the interfaces to group.
- 5 Click **Finish**.

Editing an Interface Group

- 1 From the **Firewall** menu, click **Definitions > Interfaces** tab. The Interfaces page appears.
- 2 Click the edit icon for the interface you want to edit. The Interface Group page appears.
- 3 Make your modifications and click **Finish**.

Deleting an Interface Group

- 1 From the **Firewall** menu, click **Definitions > Interfaces** tab. The Interfaces page appears.
- 2 Click the delete icon for the interface group you want to delete.

Example: Creating an Interface Group

This example creates an Interface Group named “Lan Interface”, which encompasses the LAN interfaces on a SG565 appliance.

- 1 From the **Firewall** menu, click **Definitions > Interfaces** tab. The Interfaces page appears.
- 2 Click **New**. The Interface Group page appears.

Figure 175: Interfaces selections example

Interfaces

Service Groups | Addresses | **Interfaces**

Interface Group

Name:

	Name	Details
<input type="checkbox"/>	Any Dial-In interface	
<input type="checkbox"/>	Any DMZ interface	
<input type="checkbox"/>	Any Guest interface	
<input type="checkbox"/>	Any Internet interface	
<input type="checkbox"/>	Any LAN interface	
<input type="checkbox"/>	Any VPN interface	
<input checked="" type="checkbox"/>	Switch A	LAN, Static, 192.168.0.1
<input type="checkbox"/>	Port B	Internet, Static, 10.10.57.200
<input checked="" type="checkbox"/>	WIFI (Wireless)	LAN, Static, 172.16.1.1
<input type="checkbox"/>	Lan interfaces	Switch A, WIFI

Finish **Cancel**

- 3 Enter **LAN interfaces** in the **Name** field.
- 4 Select the **Switch A** and **WIFI** check boxes.
- 5 Click **Finish**.

An action successful message is displayed, and the new interface group now appears in the Interfaces list.

Figure 176: LAN interfaces example



Packet filtering

The majority of firewall customization is typically accomplished by creating Packet Filter and NAT (Network Address Translation) rules. Packet filter rules match network packets based on a combination of incoming and outgoing interface, source and destination address, and destination port and protocol. Once a packet is matched, it can be allowed, disallowed (dropped), rejected, logged, or rate limited.

NAT rules match packets in a similar manner. However, instead of simply allowing or disallowing traffic, you can alter the source or destination address or port of the packet as it passes through the firewall. A typical use of NAT rules is to forward packets destined for your Internet IP address to an internal Web server or email server on your DMZ or LAN. Refer to “NAT” on page 245 for more information about NAT and port forwarding.

If you are creating a number of packet filter or NAT rules, it is recommended to define services (such as Web or email) and addresses (such as your internal Web server, or a trusted external host) under the Definitions menu option. You can then use these definitions in your rules, which reduces the effort and administration required for larger rule sets. For procedures on defining services, refer to the “Definitions menu” on page 198.

This section contains the following topics and procedures for packet filtering and custom firewall rules:




- “Packet Filter Rules page” on page 232
- “Creating a packet filter rule” on page 233
- “Editing a packet filter rule” on page 236
- “Disabling a packet filter rule” on page 236
- “Enabling a packet filter rule” on page 236
- “Deleting a packet filter rule” on page 236
- “Rate limiting a packet filter rule” on page 237
- “About custom firewall rules” on page 241

Packet Filter Rules page

Use this page to define rules for packet filtering. The factory default configuration includes the following predefined packet filter rules (as shown in Figure 177):

- Drop Windows Networking (enabled)
- Drop RFC1918 Incoming (disabled)
- Drop RFC1918 Outgoing (disabled)

Figure 177: Packet Filter Rules page— default rules

Packet Filter Rules									
<div>Packet Filter Rules</div> <div>Packet Filter Rules can accept, reject or drop packets based on the addresses, services, and/or interfaces. The first matching rule will determine the action for the network traffic, so the order of the rules is important.</div>									
		Descriptive Name	Action	Type	Incoming Interface	Outgoing Interface	Source Address	Destination Address	Services
<input checked="" type="checkbox"/>		Drop Windows Networking	Drop	Forward	Any	Any Internet interface	Any	Any	Windows Networking
<input type="checkbox"/>		Drop RFC1918 Incoming	Drop	Forward	Any Internet interface	Any	RFC1918	Any	Any
<input type="checkbox"/>		Drop RFC1918 Outgoing	Drop	Forward	Any	Any Internet interface	Any	RFC1918	Any

You can edit and delete the rules as necessary. If you delete all the rules on the page, the **New** button becomes available. Click **New** to define the first rule. Thereafter, you can also use the add above or add below icon to add a rule above or below an existing rule. If you use the New button, the rule is added to the bottom of the list. Use the up or down arrows to reposition a rule. For more information on icons, see “Interface icons” on page 24.

Figure 178: Packet Filter Rules page (No entries)

Packet Filter Rules									
<div>Packet Filter Rules</div> <div>Packet Filter Rules can accept, reject or drop packets based on the addresses, services, and/or interfaces. The first matching rule will determine the action for the network traffic, so the order of the rules is important.</div>									
		Descriptive Name	Action	Type	Incoming Interface	Outgoing Interface	Source Address	Destination Address	Services
No entries									
<div>New</div>									

Figure 180: Packet Filter Rule page

The screenshot shows the 'Packet Filter Rules' configuration window. It has three tabs: 'Packet Filter Rules', 'Custom Firewall Rules', and 'Custom IPv6 Firewall Rules'. The 'Packet Filter Rule' tab is active. The configuration fields are as follows:

- Descriptive Name:** A text input field.
- Enable:** A checked checkbox.
- Action:** A dropdown menu with 'None' selected.
- Type:** A dropdown menu with 'Forward' selected.
- Incoming Interface:** A dropdown menu with 'Any' selected.
- Outgoing Interface:** A dropdown menu with 'Any' selected.
- Source Address:** A dropdown menu with 'Any' selected, and a 'New' button.
- Destination Address:** A dropdown menu with 'Any' selected, and a 'New' button.
- Services:** A dropdown menu with 'Any' selected, and a 'New' button.
- Log:** An unchecked checkbox.
- Log Prefix:** A text input field.

At the bottom of the window are 'Finish' and 'Cancel' buttons.

- 3 [Optional] Enter a descriptive name in the **Descriptive Name** field.
- 4 Make sure the **Enable** check box is selected. It is enabled by default. To temporarily disable the rule, clear the check box.
- 5 From the **Action** list, select an option that specifies what to do if the rule matches. Available options are:
 - **Accept** — Allows the traffic.
 - **Drop** — Disallows the traffic and silently discards the packets. The Drop action is useful for handling packets from external untrusted hosts.
 - **Reject** — Disallows the traffic, but also sends an ICMP port unreachable message to the source IP address to advise that the packets were discarded. The Reject action is useful for packets from trusted internal hosts if you have, for example, changed the default outbound policy from allow all packets out to reject all, and then create packet filter rules for specific services and protocols that are allowed to pass traffic out of the appliance.
 - **None** — [Default] Performs no action for this rule, which is useful for a rule that logs packets but performs no other action.
- 6 The **Type** controls which incoming and outgoing interface options are available:
 - **Forward** — Filter forwarded packets only; that is, packets traversing the SnapGear appliance. You can select both incoming and outgoing interfaces.
 - **Input** — Filter packets destined for the appliance. You can only select the incoming interface.
 - **Output** — Filter packets generated by the appliance. You can only select the outgoing interface.

- 7 The **Incoming Interface** is the interface/network port on which the appliance received the network traffic. Select an option from the **Incoming Interface** list. In addition to individual interfaces and interface groups you have defined in the Definitions menu, other available options are:
 - **Any** — [Default] Select this option to match any packets received on any interface, but do not match packets originating from the appliance.
 - **None** — This option is automatically selected and displayed read-only when the **Output** option is selected in the **Type** list. This matches traffic originating from the appliance itself.
- 8 The **Outgoing Interface** is the interface/network port that the appliance routes the network traffic out of.
 - **Any** — [Default] Select this option to match packets transmitted on any interface, but do not match packets destined for this appliance.
 - **None** — This option is automatically selected and displayed read-only when the **Input** option is selected in the **Type** list. Select this option to only match packets destined for this appliance.
- 9 In the **Source Address** list, select the address that the traffic is arriving from. The options that appear in the list were defined in the Addresses page of the Definitions menu. For more information, see “Addresses page” on page 223. Default: Any. To manually enter an address, click **New**.
- 10 In the **Destination Address** list, select the address to which the traffic is destined, or click **New** to define the address. Default: Any.
- 11 If you are selecting a predefined service, go to step step 12. If you are defining a service, go to step 13.
- 12 Select a service from the **Services** list. The options that appear in the list were defined in the Services page. For more information, see “Creating a service group” on page 221.
 - a To define a service on this page, click **New**.
 - b Select an option from the **Protocol** list. This matches the protocol of the packet. Available options are:
 - **TCP**
 - **UDP**
 - **IP**
 - **ICMP**
 - c Enter one of the following to associate with the selected protocol:
 - If you selected **TCP** or **UDP** for the **Protocol**:
 - service name
 - single port number from 1-65535
 - a range of port numbers separated by hyphens
 - If you selected **IP** for the **Protocol**:
 - IP protocol number
 - If you selected **ICMP** for the **Protocol**:
 - ICMP type number

- 13 [Optional] To log the first packet of the connection to the system log, select the **Log** check box.
- 14 [Optional] To make it easier to identify which rules are being matched when inspecting the system log, enter a prefix in the **Log Prefix** field.
- 15 Click **Finish**. The rule is added to the Packet Filters Rules page. You can now move the rule up or down in the list if there are other rules already defined, or edit it to configure rate limiting. See “Rate limiting a packet filter rule” on page 237.

Editing a packet filter rule

- 1 From the **Firewall** menu, click **Packet Filtering**. The **Packet Filters Rules page** appears.
- 2 Click the edit icon for the packet filter rule you want to edit. An edit page for the rule appears.
- 3 Make your changes and click **Update**. An action successful message is displayed. Click the **Packet Filter Rules** tab to return to the main page.

Disabling a packet filter rule

- 1 From the **Firewall** menu, click **Packet Filtering**. The **Packet Filters Rules page** appears.
- 2 Click the enable check box to clear the enabled check mark. The rule is no longer enabled.

Note: You can also edit the rule and clear the **Enable** check box.

Enabling a packet filter rule

- 1 From the **Firewall** menu, click **Packet Filtering**. The **Packet Filters Rules page** appears.
- 2 Click the enable check box to select the rule. A check mark indicates the rule is enabled.

Note: You can also edit the rule and select the **Enable** check box.

Deleting a packet filter rule

- 1 From the **Firewall** menu, click **Packet Filtering**. The **Packet Filters Rules page** appears.
- 2 Click the delete icon for the packet filter rule you want to delete. You are prompted to confirm the delete. Click **OK**.

Rate limiting a packet filter rule

Once you create a packet filtering rule, you can specify rate limiting settings by editing the rule. Flood rate limiting for packet filter rules only apply to the packets associated with a rule. The rate limit must be set for each packet filter rule to which you want to apply flood rate limiting.

Rate limiting is enacted prior to the processing of its associate packet filter rule. Therefore, a rule with an allow action limits the number of connections to the service. Rate limiting is useful for preventing a service from becoming unavailable should many connection attempts occur in a short period of time, such as in the case of a denial of service (DOS) attack. Packets that exceed the specified limit can be accepted, rejected, or dropped, and can be logged.

For rules with a drop, reject, or none action, the rate limit works on all packets, unlike the rule with an allow action.

Tip: Flood rate limiting can be configured for Internet connections as well. The limiting for connections applies to all packets on all Internet connections. For further information, see “Connection tracking” on page 274.

- 1 From the **Firewall** menu, click **Packet Filtering**. The Packet Filter Rules page appears.
- 2 Click the edit icon next to the rule that you want to configure rate limiting. The edit page for the rule opens.
- 3 Click the **Rate Limit** tab. The Rate Limit tab appears.

Figure 181: Rate Limit tab

Packet Filter Rules

Packet Filter Rules | Custom Firewall Rules | Custom IPv6

Firewall Rules

Packet Filter Rule | **Rate Limit**

Rate Limit

Descriptive Name Drop RFC1918 Incoming

Enable Rate Limiting ☒

Rate (per second) 10

Burst 10

Action if Limited Reject

Log if Limited ☒

Log Prefix

Update Cancel

- 4 Select the **Enable Rate Limiting** check box.

- 5 Enter the average number of connections matched before rate limiting applies in the **Rate** (connections per second) field.
 - Default: 10
 - Accepted values: Integer equal to or greater than 1

Note: *If Access Control is enabled, then packets that traverse Access Control are rate limited separately from other packets, which means matching at potentially twice the specified rate.*

- 6 Enter the maximum instantaneous number of connections before rate limiting applies in the **Burst** field. Burst is useful for services that require multiple connections within a short time.
 - Default: 10
 - Accepted values: Integer equal to or greater than 1
- 7 Select an action to take when a packet matches the packet filter rule, but exceeds the rate limit from the **Action if Limited** list. Available options are:
 - **None** — [Default] Perform no action for rate limited packets, and continue matching on subsequent rules. This is useful if you want rate limited packets to fall through to a more general rule.
 - **Accept** — Allow the rate limited packet.
 - **Reject** — Disallow the rate limited packet, but also send an “ICMP protocol unreachable” message to the source IP address.
 - **Drop** — Silently disallow the rate limited packet.
- 8 [Optional] To log rate-limited connections, select the **Log if Limited** check box. The first packet of any-rate limited connection generates a log message.
- 9 [Optional] To ease identification of matched rules within the system log, enter an identifying string in the **Log Prefix** field. The prefix text is placed at the start of the log message.
- 10 Click **Update**.

Examples: Packet filter rules

Example 1: Creating a rule to log traffic originating from the appliance

This example creates a packet filter rule that performs no action on the packets other than to log the packets originating from the appliance. Only the first packets of the connection are logged in the syslog. This rule is useful when there is high traffic originating from the appliance when features such as access control, antivirus, and Web caching are enabled, and you want to view the level of activity from a historical perspective.

- 1 From the **Firewall** menu, click **Packet Filtering**. The Packet Filters Rules page appears.
- 2 Click **New**. The Packet Filter Rule page appears.
- 3 In the **Descriptive Name** field, enter **LogSGOutTraffic**.
- 4 Leave the **Enabled** check box selected.
- 5 From the **Action** list, select **None**.
- 6 From the **Type** list, select **Output**, since the traffic is originating from the appliance. The **Incoming Interface** now displays **None**.
- 7 Allow the **Outgoing Interface**, **Source Address**, **Destination Address**, and **Services** lists to default to the **Any** wildcard.
- 8 Select the **Log** check box, and enter **log_SG_origin_traffic** in the **Log Prefix** field.
- 9 Click **Finish**.

Example 2: Creating a rule to allow access through the appliance

This example creates a rule that allows clients on the wireless network HTTP/HTTPS access to any Web servers residing on any connected DMZ network.

Assumptions:

- There is a service defined for DMZ that consists of HTTP and HTTPS services.
- The appliance is an SG565 with a wireless interface configured.
- The wireless network is using a firewall class of Guest or Internet, as otherwise this kind of access is automatically granted anyway.
- The DNS names of the servers on the DMZ networks are publicly available on the Internet or are hard-coded.

- 1 From the **Firewall** menu, click **Packet Filtering**. The Packet Filters Rules page appears.
- 2 Click **New**. The Packet Filter Rule page appears.
- 3 In the **Descriptive Name** field, enter **wifi-to-DMZ**.
- 4 From the **Action** list, select **Accept**.
- 5 From the **Type** list, select **Forward**, since the traffic is destined to go through the appliance.
- 6 From the **Incoming Interface** list, select **WIFI (wireless)**.
- 7 From the **Outgoing Interface**, select **Any DMZ interface**.
- 8 Allow the **Source Address** and **Destination Address** lists to default to the **Any** wildcard.
- 9 In the **Services** list, select **DMZ-services**.
- 10 Click **Finish**.

About custom firewall rules

Custom firewall rules allow experts to customize the firewall configuration. The "Custom Firewall Rules tab" and "Custom IPv6 Firewall Rules tab" allow firewall experts to view the current firewall rules and add custom iptables firewall rules. Settings made within the custom firewall tabs take precedence over those configured in the Packet Filtering and NAT pages and elsewhere within the Web Management Console. Configuring the firewall using the Incoming Access and Packet Filtering pages is adequate for most applications. Only experts on firewalls and iptables should add custom firewall rules.

Note: *Secure Computing does not provide technical support for custom firewall rules.*

Further reading about firewall, NAT, and packet mangling for Linux can be found at:

<http://www.netfilter.org/documentation/>

Further reading about iptables is available at the following URL:

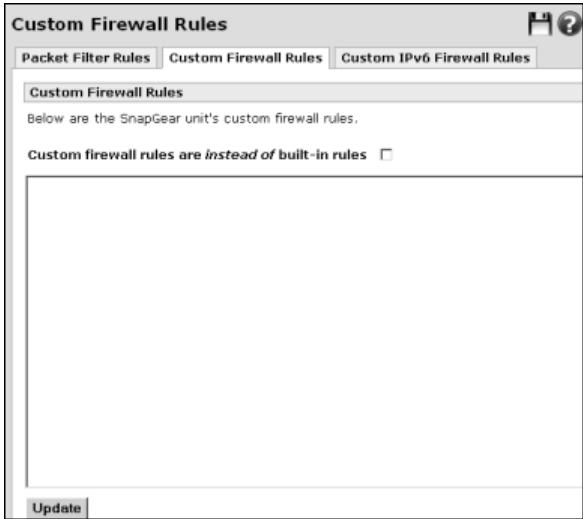
<http://iptables-tutorial.frozentux.net/>

For details on creating temporary custom log rules using iptables, refer to "Creating custom log rules" on page 546.

Custom Firewall Rules tab

This tab provides the ability to manually add custom entries to the IP tables using the iptables command syntax. The custom rules are executed whenever the status of a network interface changes. You can use custom rules either exclusively or in addition to built-in rules.

Figure 182: Custom Firewall Rules tab — upper portion



The Custom Firewall rules page also shows the iptables that are currently in effect for both built-in and custom rules. It also displays how many times each rule has been matched, which can be useful for troubleshooting. Scroll through the page to view the iptables for Packet Filter Rules, NAT Rules, and Packet Mangle Rules. A portion of the Packet Filter Rules iptables is shown in Figure 183:

Figure 183: Packet Filter Rules area

Packet Filter Rules								
Chain INPUT (policy DROP 2 packets, 307 bytes)								
pkts	bytes	target	prot	opt	in	out	source	destination
768	64512	ACCEPT	all	--	lo	*	0.0.0.0/0	0.0.0.0/0
0	0	InvalidL	all	--	*	*	0.0.0.0/0	0.0.0.0/0
2824	448K	EstabRel	all	--	*	*	0.0.0.0/0	0.0.0.0/0
6	1428	PrivIn	all	--	eth0	*	0.0.0.0/0	0.0.0.0/0
2565	417K	WanIn	all	--	eth1	*	0.0.0.0/0	0.0.0.0/0
58	6101	PrivIn	all	--	eth2	*	0.0.0.0/0	0.0.0.0/0
0	0	DefDeny	all	--	*	*	0.0.0.0/0	0.0.0.0/0

A portion of the NAT Rules iptables is shown in Figure 184:

Figure 184: NAT Rules area

NAT Rules							
Chain PREROUTING (policy ACCEPT 46262 packets, 8017K bytes)							
pkts	bytes	target	prot	opt	in	out	source
0	0	ConnFilter	tcp	--	*	*	0.0.0.0/0
Chain POSTROUTING (policy ACCEPT 18746 packets, 1617K bytes)							
pkts	bytes	target	prot	opt	in	out	source
0	0	ACCEPT	esp	--	*	*	0.0.0.0/0
0	0	ACCEPT	ah	--	*	*	0.0.0.0/0
0	0	MASQUERADE	all	--	*	eth0	0.0.0.0/0
0	0	MASQUERADE	all	--	*	eth2	0.0.0.0/0
603	24390	MASQUERADE	all	--	*	eth1	0.0.0.0/0

A portion of the Packet Mangle Rules iptables is shown in Figure 185:

Figure 185: Packet Mangle Rules area

Packet Mangle Rules							
Chain PREROUTING (policy ACCEPT 151K packets, 21M bytes)							
pkts	bytes	target	prot	opt	in	out	source
3811	542K	Filter	all	--	*	*	0.0.0.0/0
3210	484K	ConnLog	all	--	*	*	0.0.0.0/0
384	32256	CONNMARK	all	--	lo	*	0.0.0.0/0
6	1428	CONNMARK	all	--	eth0	*	0.0.0.0/0
2762	444K	CONNMARK	all	--	eth1	*	0.0.0.0/0
58	6101	CONNMARK	all	--	eth2	*	0.0.0.0/0
3210	484K	RouteIn	all	--	*	*	0.0.0.0/0
3794	539K	CONNMARK	all	--	*	*	0.0.0.0/0
3794	539K	Ts	all	--	*	*	0.0.0.0/0

To enter custom firewall rules

- 1 From the **Firewall** menu, click **Packet Filtering > Custom Firewall Rules** tab. The Custom Firewall Rules page appears.
- 2 [Optional] To use exclusively the custom rules entered in this page, select the **Custom firewall rules are instead of built-in rules** check box.
- 3 Enter the custom rules in the text box and click **Update**.

Custom IPv6 Firewall Rules tab

This tab provides the ability to manually add custom entries to the IP tables using the iptables command syntax. The custom rules are executed whenever the status of a network interface changes. You can use custom rules either exclusively or in addition to built-in rules.

The Custom Firewall rules page also shows the iptables that are currently in effect for both built-in and custom rules. It also displays how many times each rule has been matched, which can be useful for troubleshooting. Scroll through the page to view the iptables for Packet Filter and Packet Mangle Rules. NAT rules are not applicable to this page.

Figure 186: Custom IPv6 Firewall Rules tab



The screenshot shows a web interface titled "Custom IPv6 Firewall Rules". At the top, there are three tabs: "Packet Filter Rules", "Custom Firewall Rules", and "Custom IPv6 Firewall Rules". The "Custom IPv6 Firewall Rules" tab is selected. Below the tabs, there is a section titled "Custom IPv6 Firewall Rules" with the text "Below are the SnapGear unit's custom firewall rules." and a checkbox labeled "Custom firewall rules are *instead of* built-in rules" which is currently unchecked. A large text area for entering rules is below this. At the bottom left of the text area is an "Update" button. At the very bottom of the interface, there is a tab labeled "Packet Filter Rules".

To enter custom IPv6 firewall rules

- 1 From the **Firewall** menu, click **Packet Filtering > Custom IPv6 Firewall Rules** tab. The Custom IPv6 Firewall Rules page appears.
- 2 [Optional] To use exclusively the custom rules entered in this page, select the **Custom firewall rules are instead of built-in rules** check box.
- 3 Enter the custom rules in the text box.
- 4 Click **Update**.

NAT

NAT (Network Address Translation) modifies the IP address, port, or both of traffic traversing the SnapGear appliance. The appliance supports the following types of network address translation:

- **Port forwarding/Destination NAT** — For incoming traffic
- **Masquerading/Source NAT** — For outgoing traffic
- **1-to-1 NAT** — For connections established in both directions. Source and destination NAT are combined within one rule.

About port forwarding

The most common of these is *port forwarding*, which is also referred to as PAT (Port Address Translation), or DNAT (Destination NAT). This is typically used to alter the destination address (and possibly port) of matched packets arriving on the SnapGear appliance Internet interface to the address of a host on the DMZ or LAN. This is the most common way for internal masqueraded servers to offer services externally.

In Figure 187, the SnapGear appliance replaces the original destination IP address (DST_IP=3.3.3.3) of an inbound packet with the IP address of the actual DMZ server, which is 25.25.25.25. The source IP address remains the same at 1.1.1.1.

Figure 187: Port forwarding

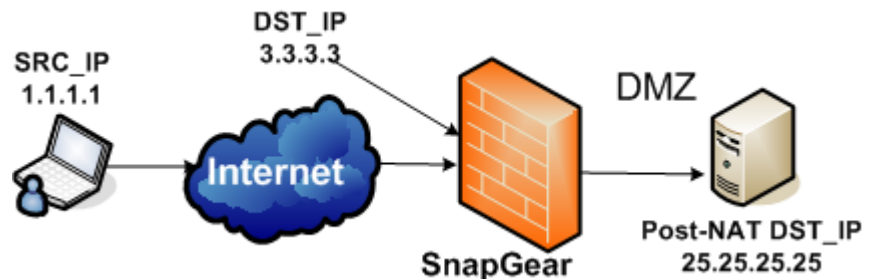


Table 15: NAT packets source and destination IP addresses

Packet from client	Packet from SnapGear after NAT
SRC_IP=1.1.1.1	SRC_IP=1.1.1.1
DST_IP=3.3.3.3 (Pre-DNAT)	DST_IP=25.25.25.25 (Post DNAT)

In the SnapGear appliance, NAT is performed as early as possible for destination addresses and as late as possible for source addresses.

About masquerading and source NAT

Source NAT rules are useful for masquerading one or more IP addresses behind a single other IP address. This is the type of NAT used by the SnapGear appliance to masquerade your private network behind its public IP address. To a server on the Internet, requests originating from the hosts behind a masqueraded interface appear to originate from the SnapGear appliance, as matched packets have their source address altered. You can enable or disable source NAT between interfaces under Masquerading, and fine tune source NAT rules under Source NAT.

Source NAT is especially useful when you have DMZ servers behind the SnapGear appliance that require having their outgoing connections they initiate appear as though they are originating from a particular public IP address. The specified public IP address would be assigned as an alias to the WAN interface of the SnapGear appliance.

In Figure 188, the SnapGear appliance replaces the source IP address (SRC_IP=1.1.1.1) packet originating with the IP address of the exiting interface, which is 3.3.3.3. The destination IP address remains 25.25.25.25.

Figure 188:
Masquerading/Source NAT

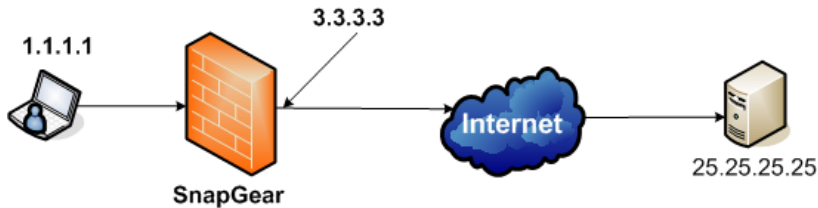


Table 16: Masquerading packets source and destination IP addresses

Packet from client	Packet from SnapGear after NAT
SRC_IP=1.1.1.1	SRC_IP=3.3.3.3
DST_IP=1.1.1.25	DST_IP=1.1.1.25

About 1-to-1 NAT

1-to-1 NAT is a combination of destination NAT and source NAT. Both destination NAT and source NAT rules are created for full IP address translation in both directions. This can be useful if you have a range of IP addresses that have been added as interface aliases on the SnapGear appliance's WAN interface, and want to associate one of these external alias IP addresses with a single internal, masqueraded computer. This effectively allocates the internal computer its own real world IP address, also known as a *virtual DMZ*. This type of NAT is used when multiple internal/DMZ servers need to be mapped to their own public IP address. The SnapGear appliance rewrites the source address on outbound packets and rewrites the destination address on inbound packets.

The NAT menu option contains the following main pages:

- “Port forwarding page” on page 248
- “Source NAT page” on page 257
- “1-to-1 NAT” on page 264
- “Masquerading page” on page 268
- “Universal Plug and Play Gateway” on page 270

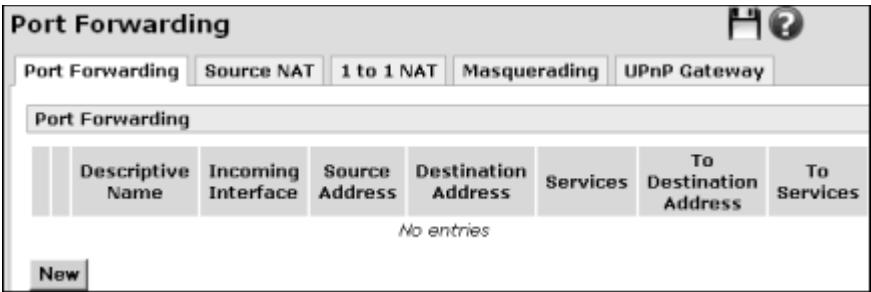
For further information on NAT, investigate the solution finder feature in the SnapGear knowledgebase (<http://sgkb.securecomputing.com>). Click the **Try a Solution Finder** tab. You can step through various configuration scenarios in the *Understanding SnapGear NAT Options* solution finder.

Port forwarding page

Port forwarding rules alter the destination address, and optionally, the destination port of packets received by the SnapGear appliance. Port forwarding allows controlled access to services provided by machines on your private network to users on the Internet by forwarding requests for a specific service coming into one of the appliance's interfaces (typically the WAN interface) to a machine on your DMZ or LAN that services the request.

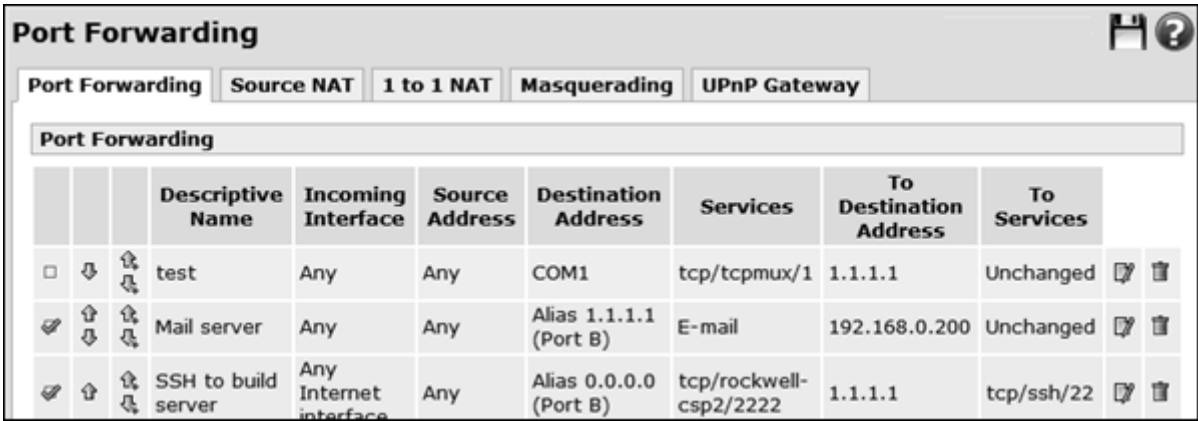
Click **New** to define the first rule, as shown in Figure 189:

Figure 189: Port Forwarding page — initial view



Thereafter, you can also use the add above or add below icon to add a rule above or below an existing rule. If you use the New button, the rule is added to the bottom of the list. Use the up or down arrows to reposition a rule. For more information on icons, see “Interface icons” on page 24. Once the page is populated with rules, you can edit and delete the rules as necessary.

Figure 190: RECAP no 0.0.0.0 Port Forwarding page — populated view



Important: Rules are evaluated from top to bottom as displayed on the page. The first matching rule determines the action for the network traffic. To reorder a rule, click the move up or down arrows.

Creating a basic port forwarding rule

Use this procedure to create a basic port forwarding rule. The rule is applied to all WAN interfaces and all source addresses are matched.

If you want to specify the incoming interface and source address for matching incoming packets, use the Advanced port forward page. In addition, if you want to disable the port forwarding rule from automatically creating a packet filtering rule, follow the advanced procedure. For instructions, refer to “Creating an advanced port forwarding rule” on page 250.

When creating a rule, you can either use predefined addresses or services or manually enter an address or service. To use the predefined definitions added through the Definitions menu, click **Show Definitions** by the fields where applicable and select a definition from the list. For more information on definitions, see “Definitions” on page 219. To manually enter an address or service, click **New**.

- 1 From the **Firewall** menu, click **NAT**. The Port Forwarding page appears.
- 2 If this is the first rule, click **New**. Otherwise, you can also click the add above or below icon to add the rule in the location you want above or below an already defined rule. The Modify Port Forward page appears.

Figure 191: Modify Port Forward (basic)

- 3 [Optional] Enter a descriptive name for the rule in the **Descriptive Name** field.
- 4 The **Enable** check box is selected by default. To temporarily disable the rule, clear the check box.

- 5 Select an address from the **Destination Address** list.
- 6 Select a protocol from the **Protocol** list. Available options are:
 - TCP
 - UDP
- 7 Enter the port or ports in the **Ports** field. If you want to show the definitions, click **Show Definitions**. The **Protocol** and **Ports** fields are replaced with the **Services** list. Select a service from the list.

Figure 192: Port Forward showing service definitions

Port Forwarding

Port Forwarding Source NAT 1 to 1 NAT Masquerading UPnP

Gateway

Modify Port Forward

Descriptive Name

Enable ☒

Match packet fields:

Destination Address Switch A (192.168.0.1)

Services Any New

Translate packet fields:

To Destination Address Show Definitions

To Services Unchanged

Finish Cancel Advanced

- 8 Enter the destination address in the **To Destination Address** field.
- 9 [Conditional; if not using definitions] Enter a port in the **Optional To Ports** field. If you select Show Definitions for the Ports field, the Optional To Ports field changes to the display-only field “To Services Unchanged”.
- 10 Click **Finish**. Make sure you create an associated packet filter rule. See “Packet filtering” on page 231.

Creating an advanced port forwarding rule

The Advanced page allows additional configuration for a port forwarding rule. You can specify the incoming interface and source address on the Advanced page; otherwise, a rule is applied to all WAN interfaces and all source addresses are matched. You can also disable the automatically created packet filter rule and manually create one that meets your specific requirements.

- 1 From the **Firewall** menu, click **NAT**. The Port Forwarding page appears.
- 2 If this is the first rule, click **New**. Otherwise, you can also click the add above or below icon to add the rule in the location you want above or below an already defined rule. If you use the New button, the rule is added to the bottom of the list. The Modify Port Forward page appears.

Figure 193: Modify Port Forward (advanced)

- 3 Click **Advanced**. The Advanced Port Forward page appears.

Port Forwarding

Port Forwarding Gateway Source NAT 1 to 1 NAT Masquerading UPnP

Modify Port Forward

Descriptive Name

Enable ☒

Create Packet Filter Rule ☒

Match packet fields:

Incoming Interface

Source Address

Destination Address

Protocol

Ports

Translate packet fields:

To Destination Address

Optional To Ports

- 4 [Optional] Enter a name for the rule in the **Descriptive Name** field.
- 5 Leave the **Enable** check box selected. To temporarily disable the rule, clear the check box.
- 6 [Optional, recommended] To create a corresponding packet filter rule to accept NATed packets, leave the **Create Packet Filter Rule** check box selected. If you want to manually create a more restrictive filter rule in the Packet Filter Rules page, clear the check box. See “Creating a packet filter rule” on page 233.

This rule is applied to packets matching the criteria described by the entries in the **Match packet fields** pane:

- 7 Select the interface that receives the request from the **Incoming Interface** list.
- 8 In the **Source Address** field, enter or select the address from which the request originated. You can specify this (rather than allowing default to Any) to restrict access of the internal service from a only specific remote location.
- 9 Select the destination address of the request from the **Destination Address** list, or click **New** to enter the address. This is the address altered by the port forwarding process.
- 10 Select the packet protocol from the **Protocol** list. Available options are:
 - TCP
 - UDP

- 11 Enter the destination service port or ports of the request in the **Ports** field. Multiple public ports can be forwarded to a single internal port.

The entries in the **Translate packet fields** pane describe how matching packets should be altered:

- 12 Enter the address to replace the Destination Address in the **To Destination Address** field. The To Destination Address is typically the private address of a host on the LAN.
- 13 Enter the translated port of the packet in the **Optional To Ports** field. Normally, this field is set to the port of a service on your internal server. Leave this blank if you want the port to remain unchanged. You can also enter the port on the host at **To Destination Address** to service the request.

Note: Ports cannot be translated for IP protocols or ICMP messages. Also, since a predefined service may contain multiple protocols, the port cannot be translated if the Services field is set to a predefined service.

- 14 Click **Finish**. The rule is added to the Port Forwarding rule objects page. If you cleared the **Create Packet Filter Rule** check box, you must create a packet filtering rule that corresponds with the port forwarding rule. See “Creating a packet filter rule” on page 233.

Editing a port forwarding rule

- 1 From the **Firewall** menu, click **NAT**. The Port Forwarding page appears.
- 2 Click the edit icon for the port forward rule you want to edit. The Modify Port Forward page appears.
- 3 Make your changes and click **Finish**.

Disabling a port forwarding rule

Use this procedure to temporarily disable a rule.

Tip: Click the enable/disable check box to the left of the object list to quickly disable the rule. The page refreshes, and the check mark is no longer displayed, indicating the rule is disabled.

- 1 From the **Firewall** menu, click **NAT**. The Port Forwarding page appears.
- 2 Clear the **Enable** check box.
- 3 Click **Finish**.

Enabling a port forwarding rule

Use this procedure to re-enable a disabled rule.

Tip: Click the enable check box to the left of the object list to quickly re-enable the rule. The page refreshes, and a check mark indicates the rule is enabled again.

- 1 From the **Firewall** menu, click **NAT**. The Port Forwarding page appears.
- 2 Click the edit icon for the port forward rule you want to edit. The Modify Port Forward page appears.
- 3 Select the **Enable** check box.
- 4 Click **Finish**.

Deleting a port forwarding rule

- 1 From the **Firewall** menu, click **NAT**. The Port Forwarding page appears.
- 2 Click the delete icon for the port forward rule you want to delete. You are prompted to confirm the delete.
- 3 Click **OK**.

Example: Basic port forwarding rule to an internal mail server

The following is an example of using port forwarding to allow mail servers on the Internet to send e-mail via SMTP to a mail server on your DMZ or LAN.



Caution: Precautions must be taken when configuring the mail server, otherwise you could become susceptible to such abuse as unauthorized relaying of unsolicited email (spam) using your server. Configuration of the e-mail server is outside the scope of this manual.

Where possible, add packet filter rules to restrict access to the internal mail server to trusted external hosts only.

- 1 First, add a service group to group email services (SMTP, POP3, and IMAP). From the **Firewall** menu, click **Definitions > Service Groups** tab > **New**.
- 2 Enter **E-Mail** in the **Name** field.

Figure 194: Modify Service Group

Service Groups

Service GroupsAddressesInterfaces

Modify Service Group

Name

E-mail

Domain (UDP)

☐

Domain (TCP)

☐

FTP

☐

HTTP (Web)

☐

HTTPS

☐

IMAP4 (E-Mail)

☒

IRC

☐

NNTP (News)

☐

NTP (Time)

☐

POP3 (E-Mail)

☒

SMTP

☒

SRMP

☐

SSH

☐

Telnet

☐

ICMP Echo Request (Ping)

☐

Other TCP Ports

Other UDP Ports

IP Protocols

ICMP Types

Finish

Cancel

- 3 Select one or both of the E-mail check boxes:
 - **IMAP4 (E-Mail)** check box if your server supports IMAP mail retrieval
 - **POP3 (E-Mail)** check box if your server supports POP3 mail retrieval.
- 4 Select the **SMTP** check box. This is the protocol remote clients use for sending mail via the server.
- 5 Click **Finish**. The e-mail service group definition is created. Next, create the port forwarding rule that uses the service group.
- 6 From the **Firewall** menu, click **NAT > Port Forwarding** tab. The Port Forwarding page appears.
- 7 If this is the first rule defined on the page, click **New**. If there are other rules already defined, click the add above or below icon to place the rule in the position you want. The Modify Port Forward page appears.
- 8 In the **Descriptive Name** field, enter **Mail server**.
- 9 Leave the **Enable** check box selected.
- 10 Select your Internet connection in the **Destination Address** field.
- 11 Next to **Ports**, click **Show Definitions**. Select **E-Mail** from the **Services** list.
- 12 Enter the IP address of your internal email server in the **To Destination Address** field. Figure 195 shows the completed page as it should appear at this step of the procedure:

Figure 195: Port forward mail server example

Port Forwarding

Port Forwarding | Source NAT | 1 to 1 NAT | Masquerading | UPnP Gateway

Modify Port Forward

Descriptive Name Mail server

Enable ☒

Match packet fields:

Destination Address Alias 1.1.1.1 (Port B)

Services E-mail **New**

Translate packet fields:

To Destination Address 192.168.0.200 **Show Definitions**

To Services Unchanged

Finish **Cancel** **Advanced**

- 13 Click **Finish**. In conjunction with DNS MX records pointing to the IP address of the SnapGear WAN, and a correctly configured internal mail server, you should now have the ability to receive SMTP mail from external hosts.

Example: Advanced port forwarding rule for SSH

This example forwards the SSH (Secure SHell) protocol to an internal server called the build server. SSH allows encrypted remote access, typically to a server running Linux, BSD, or another UNIX-like operating system. This rule uses port 2222 for SSH rather than the standard SSH port of 22. Forwarding the SSH port allows remote access using SSH to the SnapGear appliance itself, which runs an SSH server on port 22. A remote user connects to port 2222 on the SnapGear appliance's Internet address in order to access port 22 of the Build server. This example assumes there is an address defined called "Build server."

Figure 196: Port Forward for SSH example

Port Forwarding

Port Forwarding | Source NAT | 1 to 1 NAT | Masquerading | UPnP Gateway

Modify Port Forward

Descriptive Name: SSH to build server

Enable: ☒

Modify Packet Filter Rule: ☒

Match packet fields:

Incoming Interface: Any Internet interface

Source Address: Any

Destination Address: Port B (10.10. ...)

Protocol: TCP

Ports: 2222

Translate packet fields:

To Destination Address: Build server

Optional To Ports: 22

Finish | Cancel | Advanced

- 1 From the **Firewall** menu, click **NAT**. The Port Forwarding page appears.
- 2 Click the add below icon for the lowermost rule. The Modify Port Forward page appears.
- 3 Click **Advanced**. The Advanced Port Forward page appears.
- 4 In the **Descriptive Name** field, enter **SSH to Build server**.
- 5 Leave the **Enable** and **Create Packet Filter Rule** check boxes selected.
- 6 In the **Incoming Interface** field, select **Any Internet Interface**.
- 7 Allow the **Source Address** list default of **Any**.
- 8 In the **Destination Address** field, select **Port B**.

- 9 In the **Protocol** list, select **TCP**.
- 10 In the **Ports** field, enter **2222**.
- 11 In the **Destination To Address** field, enter **Build server**.
- 12 In the **Optional To Ports** field, enter **22**.
- 13 Click **Finish**.

Source NAT page

Source NAT alters the source address of packets received by the SnapGear appliance. Source NAT is typically used for fine-tuning the masquerading behavior of the appliance. For information on altering the basic masquerading relationships between your SnapGear appliance's interfaces, see "Masquerading page" on page 268.

Click **New** to define an initial rule, as shown in Figure 197:

Figure 197: Source NAT page — initial view

Source NAT							
Port Forwarding Source NAT 1 to 1 NAT Masquerading UPnP Gateway							
Source NAT							
	Descriptive Name	Outgoing Interface	Source Address	Destination Address	Services	To Source Address	To Source Ports
No entries							
New							

Thereafter, you can also use the add above or add below icon to add a rule above or below an existing rule. If you use the New button, the rule is added to the bottom of the list. Use the up or down arrows to reposition a rule. For more information on icons, see "Interface icons" on page 24. Once the page is populated with rules, you can edit and delete the rules as necessary.

Figure 198: Source NAT page—populated view

Source NAT

Port Forwarding

Source NAT

1 to 1 NAT

Masquerading

UPnP Gateway

Source NAT

		Descriptive Name	Outgoing Interface	Source Address	Destination Address	Services	To Source Address	To Source Ports
		DMZ-outbound-NAT	Port B	DMZ network	Any	Any	Alias 1.1.1.1 (Port B)	Any

New



Important: Rules are evaluated from top to bottom as displayed on the page. The first matching rule determines the action for the network traffic. To reorder a rule, click the move up or down arrow.

Creating a source NAT rule

Use this procedure to create a source NAT rule. The rule is applied to packets matching criteria described by the entries in the **Match packet** fields.

When you create a rule, you can either use predefined addresses or services or manually enter an address or service. To use the predefined definitions added through the Definitions menu, click **Show Definitions** by the fields where applicable and select a definition from the list. For more information on definitions, see “Definitions” on page 219. To manually enter an address or service, click **New**.

- 1 From the **Firewall** menu, click **NAT > Source NAT** tab.
- 2 If this is the first rule, click **New**. Otherwise, click the add above or below icon to add the rule in the location you want above or below an already defined rule. The Modify Source NAT page appears.

Figure 199: Modify Source NAT page — Predefined Services view

Source NAT

Port Forwarding Source NAT 1 to 1 NAT Masquerading UPnP Gateway

Modify Source NAT

Descriptive Name

Enable ☒

Match packet fields:

Outgoing Interface

Source Address

Destination Address

Services

Translate packet fields:

To Source Address

To Source Ports

- 3 [Optional] Enter a name for the rule in the **Descriptive Name** field.
- 4 Leave the **Enable** check box selected. To temporarily disable the rule, clear the check box.
- 5 Select the interface that the packet masquerades behind from the **Outgoing Interface** list. This matches the network interface on which the appliances transmits the packet. In addition to individual interfaces and interface groups you have defined, you can select the option **Any** to match packets that will be transmitted on any interface. You should normally set this field to your Internet interface.
- 6 Enter the address from which the request originated in the **Source Address** field. Typically, this is an IP address on an internal machine. Can be an IP address range of the following forms:
 - a.b.c.d
 - a.b.c.d-e
 - a.b.c.d-e.f.g.h
 - a.b.c.d/e
 - a.b.c.d/e.f.g.h
 - a.b.c.d+e
- 7 Enter the destination address of the request in the **Destination Address** field. This matches the destination IP address of the packet. Use this to restrict which destinations you want to use the source NAT for. The field allows the same forms as the prior step.

- 8 Enter the destination service port or ports of the request in the **Services** field. This matches the service of the packet, which may be a TCP or UDP destination port, an IP protocol, or an ICMP message type. This field allows you to use a predefined service. Or, click **New** to create a service definition when you create this rule.
- 9 [Conditional. Must have clicked **New** in step 8 to create a service definition.] Select a protocol from the **Protocol** list. This matches the protocol of the packet. Available options are:
 - TCP (default)
 - UDP
- 10 [Conditional. Must have clicked **New** in step 8 to create a service definition.] Enter a port in the **Ports** field. This matches the service of the packet, which may be a TCP or UDP destination port.
 - Can be a service name.
 - Can be a single port number from 1-65535.
 - Can be a range of port numbers in the form a-b.

The entries in the **Translate packet fields** describe how matching packets should be altered:

- 11 In the **To Source Address** field, enter the address to replace the **Source Address** with. This is typically a public address assigned as an alias to the SnapGear appliance. In addition to addresses you have predefined, the following options are also available:
 - **Unchanged**—Do not translate the source address. This is useful to prevent packets being translated by a subsequent source NAT rule.
 - **Outgoing Interface Address**—Translate the source address to the primary address of the outgoing interface.
- 12 [Conditional. Must not be using a predefined Service.] Enter the translated source port of the packet in the **Optional To Source Ports** field. Typically, you should leave this field blank. If left blank, the port is normally unchanged, but may be translated to any source port if required.
 - Can be a service name.
 - Can be a single port number from 1-65535.
 - Can be a range of port numbers in the form a-b.

Note: You cannot translate the port for IP protocols or ICMP messages. In addition, you cannot translate the source port if Services is set to a predefined Service. Since a predefined service may contain multiple protocols, a single port definition is not well-defined.

- 13 Click **Finish**.

Figure 200: Modify Source NAT page — Define Protocol and Ports view

Source NAT

Port Forwarding | **Source NAT** | 1 to 1 NAT | Masquerading | UPnP Gateway

Modify Source NAT

Descriptive Name

Enable ☒

Match packet fields:

Outgoing Interface

Source Address

Destination Address

Protocol

Ports

Translate packet fields:

To Source Address

Optional To Source Ports

Editing a source NAT rule

- 1 From the **Firewall** menu, click **NAT > Source NAT** tab.
- 2 Click the edit icon for the rule you want to edit. The Modify Source NAT page appears.
- 3 Make your changes and click **Finish**.

Disabling a source NAT rule

Use this procedure to temporarily disable a rule.

Tip: Click the enable/disable check box to the left of the object list to quickly disable the rule. The page refreshes, and the check mark is no longer displayed, indicating the rule is disabled.

- 1 From the **Firewall** menu, click **NAT > Source NAT** tab. The Source NAT page appears.
- 2 Clear the **Enable** check box.
- 3 Click **Finish**.

Enabling a source NAT rule

Use this procedure to re-enable a disabled rule.

Tip: Click the enable check box to the left of the object list to quickly re-enable the rule. The page refreshes, and a check mark indicates the rule is enabled again.

- 1 From the **Firewall** menu, click **NAT > Source NAT** tab. Any rules that have already been defined are displayed.
- 2 Click the edit icon for the rule you want to edit. An edit page appears.
- 3 Select the **Enable** check box.
- 4 Click **Finish**.

Deleting a source NAT rule

- 1 From the **Firewall** menu, click **NAT > Source NAT** tab.
- 2 Click the delete icon for the rule you want to delete. You are prompted to confirm the delete. Click **OK**.

Example: Creating a source NAT rule

This example defines a unique NAT address to use for outbound packets originating from the DMZ network.

This example assumes there are address definitions defined for Port B named “Internet (Port B)”, an address defined for the DMZ named “DMZ-network”, and an address defined named “Internet-Alias” to translate the IP address. For information on defining addresses, see “Adding an IP address or range” on page 223.

- 1 From the **Firewall** menu, click **NAT > Source NAT** tab.
- 2 In the **Descriptive Name** field, enter **DMZ-outbound-NAT**.
- 3 In the **Outgoing Interface** list, select **Internet (Port B)**.
- 4 In the **Source Address** list, select the **DMZ-network** definition.
- 5 In the **To Source Address** list, select the **Internet-Alias** definition.
- 6 Click **Finish**. All packets originating from the DMZ network will have their source addresses altered to the IP address defined for “Internet-Alias”.

Figure 201: Source NAT example

The screenshot shows the 'Source NAT' configuration window. At the top, there are tabs for 'Port Forwarding', 'Source NAT' (which is selected), '1 to 1 NAT', 'Masquerading', and 'UPnP Gateway'. Below the tabs is a section titled 'Modify Source NAT'. It contains the following fields and options:

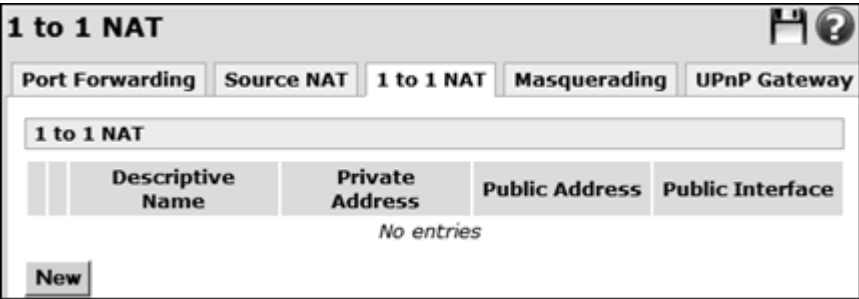
- Descriptive Name:** A text box containing 'DMZ-outbound-NAT'.
- Enable:** A checkbox that is checked.
- Match packet fields:** A section with three dropdown menus:
 - Outgoing Interface:** Set to 'Internet (Port B)'.
 - Source Address:** Set to 'DMZ-network'.
 - Destination Address:** Set to 'Any'.
- Services:** A dropdown menu set to 'Any'.
- Translate packet fields:** A section with two dropdown menus:
 - To Source Address:** Set to 'Internet-Alias'.
 - To Source Ports:** Set to 'Any'.

At the bottom of the window are two buttons: 'Finish' and 'Cancel'.

1-to-1 NAT

The 1 to 1 NAT creates both a source NAT and destination NAT rule for mapping all services on an internal private address to an external public address and vice-versa. This form of NAT maps an external public address to an internal private address.

Figure 202: 1 to 1 NAT
page—initial view



Important: Rules are evaluated from top to bottom as displayed on the page. The first matching rule determines the action for the network traffic. To reorder a rule, click the move up or down arrows.

Creating a 1 to 1 NAT rule

Use this procedure to create a 1-to-1 NAT rule. After you add a 1-to-1 NAT rule, you must manually create packet filter rules to allow external users access to the internal private address, if required. For more information, see “Creating a packet filter rule” on page 233.

When creating a rule, you can either use predefined addresses or services or manually enter an address or service. To use the predefined definitions added through the Definitions menu, click **Show Definitions** by the fields where applicable and select a definition from the list. For more information on definitions, see “Definitions” on page 219. To manually enter an address or service, click **New**.

- 1 From the **Firewall** menu, click **NAT > 1 to 1 NAT** tab. The 1 to 1 NAT page appears.
- 2 If this is the first rule, click **New**. Otherwise, click the add above or below icon to add the rule in the location you want above or below an already existing rule. The Modify 1 to 1 NAT tab appears.

Figure 203: 1 to 1 NAT

1 to 1 NAT

Port Forwarding Source NAT **1 to 1 NAT** Masquerading UPnP Gateway

Modify 1 to 1 NAT

Descriptive Name

Enable ☒

Private Address

Public Address

Public Interface

- 3 [Optional] Enter a **Descriptive Name**.
- 4 [Optional] The **Enable** check box is selected by default. If you do not want to enable the rule at this time, clear the check box.
- 5 Enter the private address to change in the **Private Address** field.
- 6 Enter the public address, typically a WAN interface alias, in the **Public Address** field.
- 7 Select the interface on which the public address reside from the **Public Interface** list. Typically, this is Internet.
- 8 Click **Finish**. The rule is added to the main 1 to 1 NAT rule page. Make sure you add a corresponding packet filter rule. See “Creating a packet filter rule” on page 233.

Editing a 1-to-1 NAT rule

- 1 From the **Firewall** menu, click **NAT > 1 to 1 NAT** tab. The 1 to 1 NAT page is displayed. Any rules that have already been defined are displayed.
- 2 Click the edit icon for the rule you want to edit. An edit page appears.
- 3 Make your changes and click **Finish**.

Disabling a 1-to-1 NAT rule

Tip: Click the enable/disable check box to the left of the object list to quickly disable the rule. The page refreshes, and the check mark is no longer displayed, indicating the rule is disabled.

- 1 From the **Firewall** menu, click **NAT > 1 to 1 NAT** tab. The 1 to 1 NAT page is displayed. Any rules that have already been defined are displayed.
- 2 Click the edit icon for the rule you want to edit. An edit page appears.
- 3 Clear the **Enabled** check box.
- 4 Click **Finish**.

Enabling a 1-to-1 NAT rule

Use this procedure to re-enable a disabled rule.

Tip: Click the enable check box to the left of the object list to quickly re-enable the rule. The page refreshes, and a green check mark indicates the rule is enabled again.

- 1 From the **Firewall** menu, click **NAT > 1 to 1 NAT** tab. The 1 to 1 NAT page is displayed. Any rules that have already been defined are displayed.
- 2 Click the edit icon for the rule you want to edit. An edit page appears.
- 3 Select the **Enable** check box.
- 4 Click **Finish**.

Deleting a 1-to-1 NAT rule

- 1 From the **Firewall** menu, click **NAT > 1 to 1 NAT** tab. Any rules that have already been defined are displayed.
- 2 Click the delete icon for the rule you want to delete. You are prompted to confirm the delete. Click **OK**.

Example: Creating a 1-to-1 NAT rule

This example creates a rule to map the private address of the mail server on the LAN to a public IP address on the Internet Interface, Port B.

This example assumes there is a predefined address named “LAN-Mail-Server”, and an address alias 1.1.1.1 defined for port B.

- 1 From the **Firewall** menu, click **NAT > 1 to 1 NAT** tab. The 1 to 1 NAT page is displayed. Any rules that have already been defined are displayed.
- 2 Click **New**, or the add above or below icon, depending on your current configuration and where you want to place the rule. The Modify 1 to 1 NAT page appears.
- 3 In the **Descriptive Name** field, enter **LAN-Mail-Server-NAT**.
- 4 Allow the **Enable** check box to remain selected.
- 5 From the **Private Address** list, select **LAN-Mail-Server**.
- 6 From the **Public Address** list, select **Alias (ip address) Port B**.
- 7 From the **Public Interface** list, select **Port B**.
- 8 Click **Finish**.

Figure 204: 1 to 1 NAT example

The screenshot shows the '1 to 1 NAT' configuration window. At the top, there are tabs for 'Port Forwarding', 'Source NAT', '1 to 1 NAT' (which is selected), 'Masquerading', and 'UPnP Gateway'. Below the tabs is a section titled 'Modify 1 to 1 NAT'. This section contains the following fields and controls:

- Descriptive Name:** A text field containing 'LAN-Mail-Server-NAT'.
- Enable:** A checked checkbox.
- Private Address:** A dropdown menu showing 'LAN-Mail-Server' with a 'New' button to its right.
- Public Address:** A dropdown menu showing 'Alias 1.1.1.1 (Port B)' with a 'New' button to its right.
- Public Interface:** A dropdown menu showing 'Port B'.
- At the bottom of the section are 'Finish' and 'Cancel' buttons.

Masquerading page

Masquerading is a form of source NAT. It translates many addresses, such as private LAN IP addresses, into a single address, such as the external IP address. Masquerading has the following advantages:

- All machines on the local network can access the Internet using a single ISP account.
- Only one public IP address is used and is shared by all machines on the local network. Each machine has its own private IP address.

The firewall remains active when masquerading is disabled. If you require a finer level of control, such as enabling or disabling masquerading for a single port, then you should use Source NAT. Refer to “Source NAT page” on page 257.

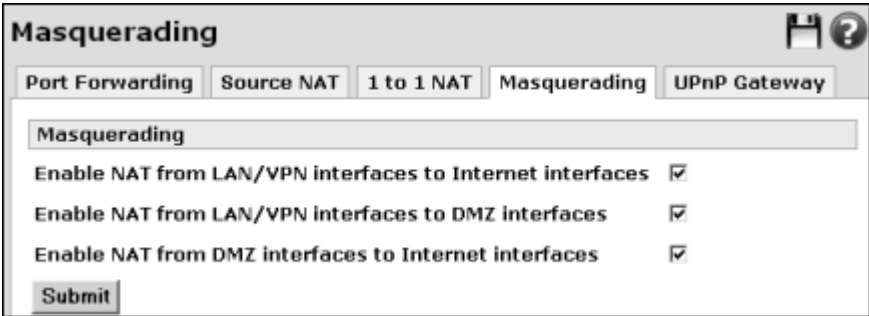
The default configuration for the SnapGear appliance automatically protects your internal private IP addresses by masquerading them to the IP address of the appliance’s Internet interface. The Masquerading tab provides high-level controls to enable masquerading between types of network interfaces.

Note: The displayed options apply to the firewall classes. The LAN interface options apply to all interfaces that are configured with a LAN connection type. For NAT purposes, the Guest connection is considered a LAN interface.

Enabling masquerading

- 1 Click **Firewall > NAT > Masquerading**. The Masquerading page appears.

Figure 205:
Masquerading page



- 2 Leave the **Enable NAT from LAN/VPN interfaces to Internet interfaces** check box selected. Typically, this is required to allow Internet access from the LAN. If you are using a private IP address range on your LAN (for example 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16), then you probably want to keep this option enabled.

Note: Disable this option only if you have publicly routeable IP addresses on your LAN, which is generally not recommended.

- 3 [Enabled by default] To enable masquerading for connections between any LAN interface and any DMZ interface, select the **Enable NAT from LAN/VPN interfaces to DMZ interfaces** check box. Disable this option only if you want to route traffic instead between the LAN/VPN to DMZ interfaces.
- 4 [Recommended, enabled by default] To enable masquerading for connections between any DMZ interface and any WAN interface, select the **Enable NAT from DMZ interfaces to Internet interfaces** check box. Disable this option only if you have publicly routeable IP address on your DMZ.
- 5 Click **Submit**.

Disabling masquerading

If you disable masquerading, the SnapGear appliance simply routes packets instead, which might be desired in certain environments.

- 1 Click **Firewall > NAT > Masquerading**.
- 2 Clear the check boxes for the interfaces for which you want to disable masquerading.



Important: To allow Internet access from the LAN, leave the **Enable NAT from LAN/VPN interfaces to Internet interfaces** check box selected.

- 3 Click **Submit**.

Universal Plug and Play Gateway

The UPnP (Universal Plug and Play) Gateway allows UPnP-capable applications and devices to request port forwarding rules to be established on demand. This allows some applications and devices that might not operate correctly behind the NAT firewall to automatically work.



Caution: When UPnP is enabled, any host connected to the internal network can create a port-forwarding rule on the firewall. Secure Computing strongly recommends you do not enable the UPnP Gateway feature.

The UPnP Gateway needs to be run on a pair of interfaces: the external interface (typically default gateway internet) and the internal interface (typically LAN or DMZ). The UPnP Gateway sends out notifications on the internal interface, advertising its presence on the network. Any UPnP-capable applications or devices you require to make use of the UPnP Gateway need to be connected to the SnapGear appliance via this interface. The UPnP Gateway listens on this interface to requests from UPnP-capable applications and devices to establish port forwarding rules. In response to these requests, the UPnP Gateway establishes port forwarding rules to allow matching packets to be forwarded from the configured external interface through to the internal interface.

The port forwarding rules set up via the UPnP Gateway are temporary. The list of configured UPnP port forwarding rules is cleared should the SnapGear appliance be power cycled, or should the internal or external interface become unavailable. The UPnP Gateway is intended for transitory application port forwarding, such as those established by some versions of Microsoft Messenger for file transfers. For long term port forwarding, configuring the necessary rules via the Destination NAT features in Packet Filtering is recommended. Should there be a conflict; packet filtering and NAT rules take precedence over UPnP rules.

Enabling and configuring the UPnP Gateway

- 1 From the **Firewall** menu, click **NAT > UPnP Gateway** tab. The UPnP Gateway page appears.

Figure 206: UpnP Gateway page

UPnP Gateway

Port Forwarding Source NAT 1 to 1 NAT Masquerading **UPnP Gateway**

UPnP Configuration

The Universal Plug and Play (UPnP) Gateway allows UPnP-aware applications and operating systems to request port forwarding rules to be established on demand. This allows some applications that may not operate correctly behind the NAT firewall to automatically work.

Note, there is concern in the security community over the potential vulnerability that UPnP Gateways present. For maximum security disable the UPnP Gateway feature.

Enable UPnP Gateway ☐

Internal Interface

External Interface

Enable verbose syslog information ☐

Submit

Current UPnP Port Mappings

Protocol	Port	Target
No entries		

Refresh

- 2 [Optional] Select the **Enable UPnP Gateway** check box.
- 3 Select an interface from the **Internal Interface** list.
- 4 Select an interface from the **External Interface** list.
- 5 [Optional] To enable detailed syslog information for UPnP activities, select the **Enable verbose syslog information** check box. You can view details of every UPnP transaction carried out by the UPnP Gateway recorded in the system log.
- 6 Click **Submit**.

Configuring UPnP rules from Windows XP

Once UPnP is running on the SnapGear appliance, you can configure UPnP port forwarding rules from a local Windows XP PC.

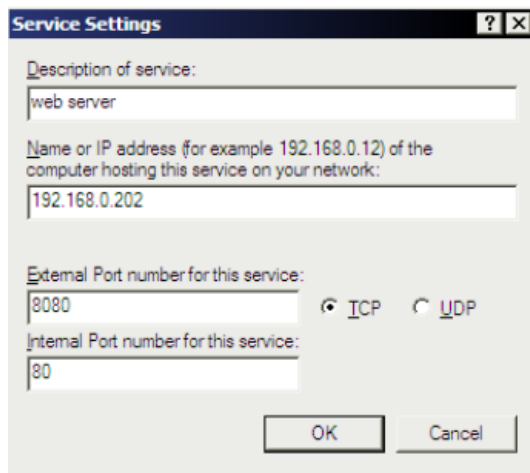
- 1 Ensure the PC's **Default gateway** is set to the SnapGear appliance's UPnP **Internal interface**.
- 2 After 10 to 15 seconds, a new connection named **Internet Connection** appears in the PC's **Network Connections** folder.

Figure 207: Network Connections



- 3 Open **Internet Connection**, click **Settings > Add**.

Figure 208: Service Settings



- 4 Enter an arbitrary **Description of service**.
- 5 Enter the **Name or IP address of the computer hosting this service on your network**.

- 6 Enter the **External Port** number for this service.
- 7 Enter the **Internal Port** number for this service.
- 8 Select whether the service uses the **TCP** or **UDP** protocol.
- 9 Click **OK**.

Figure 209: Current UPnP Port Mappings

Current UPnP Port Mappings		
Protocol	Port	Target
tcp	8080	192.168.0.202:80
Refresh		

This rule now appears on the SnapGear appliance UPnP page in the **Current UPnP Port Mappings** pane.

Viewing and refreshing UPnP port forwards

Use this procedure to view and refresh UPnP port forwarding information. The UPnP Gateway page shows a list of all the UPnP port forwards currently established on the device.

Prerequisite: You must configure UPnP rules on a local Windows PC. See “Configuring UPnP rules from Windows XP” on page 272.

- 1 From the **Firewall** menu, click **NAT > UPnP Gateway** tab. The UPnP Gateway page appears.
- 2 Click **Refresh**. The page displays the current UPnP status:
 - **Protocol:** This column shows the transport layer protocol for which the UPnP port forward is established. Either TCP or UDP.
 - **Port:** This column shows the incoming port on which the forward has been established. Packets with a matching protocol arriving at this port on the configured external interface will be accepted and forwarded.
 - **Target:** This column shows the destination address of packets that have been port forwarded. Takes the form of: *target IP address:port number*.

Connection tracking

Connection tracking keeps a record of packets that have passed through the appliance and how they relate to each other. A sequence of related packets is called a *connection*, which is required for stateful packet filtering and network address translation (NAT). Most packets are correctly handled by generic support for protocols such as TCP and UDP. However, some services or protocols are more complicated in that they make multiple connections for a session, and therefore require specific connection tracking modules in order to record the state correctly. For example, FTP requires additional connections for data transfer, and also transmits IP addresses and ports within the data portion of packets.

The SnapGear appliance supports connection tracking for the following protocols:

- **FTP** – File Transfer Protocol
- **H.323** – Video, audio conferencing
- **IRC** – Internet Relay Chat
- **PPTP** – Point to Point Tunneling Protocol
- **TFTP** – Trivial File Transfer Protocol

The appliance tracks the initial connection allowed, and then looks for secondary connections that are established. Without connection tracking for FTP, only the control channel connection is allowed through; Active Mode data channels are dropped. Without Connection Tracking for PPTP, only the control connection on port 1723 is allowed; the GRE traffic is dropped.

To reiterate, connection tracking applies to *all* services allowed through the firewall, not just to the specific protocols listed above.

Connection logging

Connection tracking can log all connections passing through the firewall. You can enable connection logging for the start and end of every connection. Connection logging can be useful if you have a log analyzer to parse the log for purposes such as accounting or intrusion detection. Each log entry specifies the connection ID, protocol, source and destination addresses and ports, protocol, number of packets, and number of bytes. These are specified for both the original direction and the reply direction. The addresses for the original direction are before NAT, and the addresses for the reply direction are after NAT.

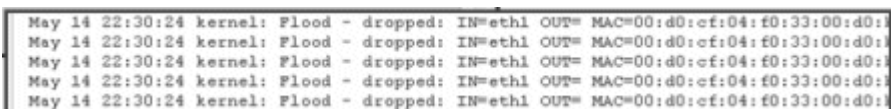
Tip: Connection logging generates a large number of entries in the system log, and should only be used if you have enabled remote logging on the Remote Syslog page. For more information, refer to “Enabling remote system logging” on page 501.

Preventing connection flooding

Connection tracking can limit the connection rate on the Internet interface, which prevents connection flooding.

The connection rate is measured in connections per second. A connection is considered to be new if its source, destination, and other parameters cannot be matched to a connection already in the connection tracking table. When connections exceed the rate limit, the SnapGear appliance assumes it is being attacked and logs either “Flood” or “SynFlood” in the system log, as shown in Figure 210:

Figure 210: Logged flood rate limiting



```
May 14 22:30:24 kernel: Flood - dropped: IN=eth1 OUT= MAC=00:d0:cf:04:f0:33:00:d0:1
May 14 22:30:24 kernel: Flood - dropped: IN=eth1 OUT= MAC=00:d0:cf:04:f0:33:00:d0:1
May 14 22:30:24 kernel: Flood - dropped: IN=eth1 OUT= MAC=00:d0:cf:04:f0:33:00:d0:1
May 14 22:30:24 kernel: Flood - dropped: IN=eth1 OUT= MAC=00:d0:cf:04:f0:33:00:d0:1
```

For security, the SnapGear appliance drops incoming connections that exceed the flood rate limit.

This section contains the following topics:

- “Configuring connection tracking” on page 276
- “About the Connection Tracking Report” on page 278
- “Viewing the connection tracking report in the console” on page 281
- “Downloading the connection tracking report” on page 282
- “Example: Creating a connection tracking report” on page 283

Configuring connection tracking

Use this procedure to configure connection tracking. By default, all modules are enabled for connection tracking. Since connection tracking modules can allow additional connections through the firewall, you should disable modules you do not need.

Implementations of protocols such as H.323 can vary, so if you are experiencing problems, try disabling the H.323 module. Disabling H.323 might be necessary when using H.323 across links that do not perform NAT, such as IPSec or PPTP tunnels.

You can view connection tracking details in the connection tracking report. For more information, see “About the Connection Tracking Report” on page 278.

- 1 From the **Firewall** menu, click **Connection Tracking**. The Connection Tracking page appears.

Figure 211: Connection Tracking page

Enabled	Module	Description
<input checked="" type="checkbox"/>	ftp	File transfer protocol (FTP)
<input checked="" type="checkbox"/>	h323	H.323 teleconferencing
<input checked="" type="checkbox"/>	irc	Internet relay chat (IRC)
<input checked="" type="checkbox"/>	pptp	Point-to-point tunneling protocol (PPTP)
<input checked="" type="checkbox"/>	tftp	Trivial file transfer protocol (TFTP)

Enable Connection Logging ☒

Enable Flood Rate Limiting ☒

Flood Rate Limit (per second)

- 2 Select the **Enabled** check box for the Modules you need to track. Clear the Enabled check box for the modules you do not need to track. Disabling a module disallows any additional connections through the firewall as a result of connection tracking. Available modules are:
 - **FTP**
 - **H.323**
 - **IRC**
 - **PPTP**
 - **TFTP**

- 3 [Optional] Select the **Enable Connection Logging** check box to log connections to the system log as they are established and expire; however, this can result in excessive log messages if you have a large or busy network. Make sure you have enabled remote system logging if you enable connection logging. See “Enabling remote system logging” on page 501.
- 4 [Optional] To enable flood rate limiting for new connections on Internet interfaces, select the **Enable Flood Rate Limiting** check box. Attempts to initiate new connections that exceed the defined rate limit are logged and dropped.
- 5 [Conditional; required for Enabled Flood Rate Limiting] Enter an integer value equal to or greater than 1 in the **Flood Rate Limit (per second)** field. This is the number of connections per second to allow before dropping new connections. If you are port forwarding to a busy internal server, increase or disable the Flood Rate Limit setting as needed.
- 6 Click **Submit**.

About the Connection Tracking Report

Use this report to view information about the current connections to a SnapGear appliance. The connection information tracked in this report is configured in the Connection Tracking Configuration page (see Figure 211 on page 276). The information you want to view within the report is configured within this Report Configuration page.

Prerequisite: Connection logging must be enabled. See “Configuring connection tracking” on page 276.

Figure 212: Connection Tracking Report

Connection Tracking

Configuration Report

Connection Tracking Report

Report Configuration:

Fields	Display	Filter
Protocol	<input type="checkbox"/>	
Connection State	<input checked="" type="checkbox"/>	
Connection Timeout	<input type="checkbox"/>	
Src IP	<input checked="" type="checkbox"/>	
Dest IP	<input checked="" type="checkbox"/>	
Src Port	<input type="checkbox"/>	
Dest Port	<input type="checkbox"/>	
Packets	<input type="checkbox"/>	
Bytes	<input type="checkbox"/>	
Reply Src IP	<input type="checkbox"/>	
Reply Dest IP	<input type="checkbox"/>	
Reply Src Port	<input type="checkbox"/>	
Reply Dest Port	<input type="checkbox"/>	
Reply Packets	<input type="checkbox"/>	
Reply Bytes	<input type="checkbox"/>	
Routing Interface	<input checked="" type="checkbox"/>	

Sort by (Ascending) No sorting

Maximum display rows 20

System processing limit 3911

View Details Download Details

You can select the **Display** check boxes to indicate which fields you want to include in a report. The **Filter** box is available for additional narrowing of your reporting criteria. You can optionally sort a specified column in ascending order using the **Sort by (Ascending)** list.

The **View Details** button displays the report directly within the Connection Tracking Report page, at the bottom of the page. If you are viewing the report within the console, you can limit the number of rows you want to view within a report by entering a value in the **Maximum display rows** field.

You can also opt to download the report to a text file with the **Download Details** button. If you download a report, all data is downloaded since the maximum rows value is ignored and there are no limitations applied to the number of rows.

Connection State Field

This is the key field within the report that details the current state of a connection. The Connection State field has the following format within the report:

[TCP_State],[Seen_Reply],[Assured]

TCP_State—is blank for all protocols except TCP. Examples include TIME_WAIT and ESTABLISHED.

Seen_Reply—is either blank or [UNREPLIED] if the appliance has not received an expected reply.

Assured—is either blank or [ASSURED] when multiple request and replies have occurred between the same socket pairs.

Fields applicable to TCP or UDP protocol only

The following fields are only applicable for connections using TCP or UDP protocol:

- **Src port**—Source Port
- **Dest Port**—Destination Port
- **Reply Src Port**—Reply Source Port
- **Reply Dest Port**—Reply Destination Port

Available filter types

Table 17: Connection tracking report filters

Fields	Filter Type
Protocol	Case-sensitive string
Connection State	Case-sensitive string
Source IP	Case-sensitive string
Destination IP	Case-sensitive string
Source Port	Numeric match
Destination Port	Numeric match
Reply Source IP	Case-sensitive string
Reply Destination IP	Case-sensitive string
Reply Source Port	Numeric match
Reply Destination Port	Numeric match
Routing Interface	Case-sensitive string

Viewing the connection tracking report in the console

Use this procedure to view the report directly within the Web management console.

- 1 Click **Connection Tracking > Report** tab. The Connection Tracking Report page is displayed.
- 2 Select the **Display** check box for the fields you want to include in the report.
- 3 [Optional] If available for a field, enter any additional filter criteria in the **Filter** field.
- 4 [Optional] Select a column you want to sort from the **Sort by** list. The list contains all of the fields in the report.
- 5 Enter the maximum number of rows you want displayed in the **Maximum display rows** field. This value cannot exceed the display-only value shown in the **System processing limit** field. The system limit value is dynamic depending on your current selections.
 - Default: 20
- 6 Click **View Details**. An action successful message is displayed. You can click the **Displaying current connection details [here](#)** link to jump to the bottom of the page where the results are displayed, or use the scroll bars.

Figure 213: Current Connection Details

Current Connection Details				
As at: Mon Feb 12 16:38:58 2007 CST Displaying first 20 of 24 matching current connection details.				
Protocol	Connection State	Connection Timeout	Src IP	Dest IP
udp	,[UNREPLIED],	5	10.10.65.91	10.10.255.255
udp	,[UNREPLIED],	10	10.10.75.77	10.10.255.255
udp	,[UNREPLIED],	22	10.10.1.189	10.10.255.255
udp	,[UNREPLIED],	13	10.10.36.84	10.10.255.255
udp	,[UNREPLIED],	0	10.10.17.6	10.10.255.255
udp	,[UNREPLIED],	9	10.10.16.92	10.10.255.255
udp	,[UNREPLIED],	3	10.10.209.17	10.10.255.255
udp	,[UNREPLIED],	15	10.10.207.1	10.10.255.255
udp	,[UNREPLIED],	29	10.10.75.77	10.10.255.255

Downloading the connection tracking report

Use this procedure to download the connection tracking report rather than viewing it directly within the console. The download creates a tab-delimited file you can either view in an associated text editor such as Notepad, or save for importing into a spreadsheet application such as Excel for further sorting.

When you download report details, all matching details are output to the report. The Sort By and Maximum Rows values are ignored.

- 1 Click **Connection Tracking > Report** tab. The Connection Tracking Report page is displayed.
- 2 Select the **Display** check box for the fields you want to include in the report.
- 3 [Optional] If available for a field, enter any additional filter criteria in the **Filter** field.
- 4 [Optional] Select a column you want to sort from the **Sort By** list. The Sort By list contains all of the fields in the report. Default: No sorting.
- 5 Enter the maximum number of rows you want displayed in the **Maximum display rows** field. This value cannot exceed the display-only value shown in the **System processing limit** field. The system limit value is dynamic depending on your current selections.
 - Default: 20
- 6 Click **Download Details**. The File Download dialog box is displayed.
- 7 Click **Open** to view the text file directly, or click **Save** to save the file. The default filename contains the date and current time of the report.

Example: Creating a connection tracking report

This example creates a connection tracking report that focuses on source and destination IP addresses and their associated routing interface.

- 1 Click **Connection Tracking > Report** tab. The Connection Tracking Report page is displayed.
- 2 Select the **Display** check boxes for the **Src IP**, **Dest IP**, and **Routing Interface** fields. Clear all other check boxes.
- 3 Click **View Details**. The report is displayed in the lower half of the page. You can see the source IP addresses currently connected. The current date and time is given, along with connections matching your selection criteria.

Figure 214: Current Connection Details

Current Connection Details			
As at: Tue Mar 20 16:00:51 2007 CDT			
Displaying 4 of 4 matching current connection details.			
Connection State	Src IP	Dest IP	Routing Interface
„[ASSURED]	10.10.57.200	10.10.1.254	eth1
,[UNREPLIED],	10.10.57.200	100.1.1.99	eth1
,[UNREPLIED],	192.168.0.1	192.168.0.255	eth0.2
ESTABLISHED„[ASSURED]	172.16.1.101	172.16.1.1	eth2

Intrusion Detection Systems

Note: The SG300 and SG560 provide Basic Intrusion Detection and Blocking only.

The SnapGear appliance provides two IDS (Intrusion Detection Systems):

- Lightweight and simple-to-configure Basic IDB (Intrusion Detection and Blocking)
- Industrial-strength Advanced Intrusion Detection and Prevention

These two systems take quite different approaches. Basic Intrusion Detection offers a number of dummy services to the outside world, which are monitored for connection attempts. Clients attempting to connect to these dummy services can be blocked. Advanced Intrusion Detection uses complex rule sets to detect known methods used by intruders to circumvent network security measures, which it either blocks or logs to a remote database for analysis.

Benefits of using an IDS

External attackers attempting to access desktops and servers on the private network from the Internet are the largest source of intrusions. Attackers exploiting known flaws in operating systems, networking software, and applications compromise many systems through the Internet.

Generally firewalls are not granular enough to identify specific packet contents that signal an attack based on a known system exploit. Firewalls act as a barrier analogous to a security guard screening anyone attempting to enter and dismissing those deemed unsuitable, based on criteria such as identification. However, identification can be forged. On the other hand, intrusion detection systems are more like security systems with motion sensors and video cameras. Video screens can be monitored to identify suspect behavior and help to deal with intruders.

Firewalls often easily bypassed through well-known attacks. The most problematic types of attacks are tunneling-based and application-based. Tunneling-based attacks occur when an attacker masks traffic normally screened by the firewall rules by encapsulating it within packets corresponding to another network protocol. Application-based attacks occur when vulnerabilities in applications can be exploited by sending suspect packets directly with those applications. These attacks can potentially be detected and prevented using an intrusion detection system.

Basic IDB

Basic IDB operates by offering a number of services to the outside world that are monitored for connection attempts. Remote machines attempting to connect to these services generate a system log entry providing details of the access attempt, and the access attempt is denied. Since network scans often occur before an attempt to compromise a host, you can also deny all access from hosts that have attempted to scan monitored ports.

Note: An attacker can easily forge the source address of UDP or TCP requests. A host that automatically blocks UDP or TCP probes might inadvertently restrict access from legitimate services. Proper firewall rules and ignored hosts lists significantly reduce the risk of restricting legitimate services.

Configuring basic IDB

- 1 From the **Firewall** menu, click **Intrusion Detection**. The IDB Configuration page appears.

Figure 215: IDB Configuration

IDB Configuration

IDB Snort IPS

IDB TCP UDP

IDB Configuration

Detect TCP probes ☐

Block sites probing TCP ports ☐

Detect UDP probes ☐

Block sites probing UDP ports ☐

Trigger count before blocking

Addresses to ignore for detection and blocking purposes

0.0.0.0
127.0.0.1

Submit

Scanning Hosts

Hosts which have been detected as scanning the monitored ports of this host and which have been barred access are listed below. In each case, the probe which resulted in the blocking is shown.

Host	Detected	Protocol	Port
No entries			

- 2 [Optional] To monitor dummy TCP services, select the **Detect TCP probes** check box.
- 3 [Optional] To blocks hosts attempting to connect to TCP services, select the **Block sites probing TCP ports** check box. Connection attempts are logged under the **Scanning Hosts** pane.
- 4 [Optional] To monitor dummy UDP services, select the **Detect UDP probes** check box.
- 5 [Optional] To blocks hosts attempting to connect to UDP services, select the **Block sites probing UDP ports** check box. Connection attempts are logged under **Scanning Hosts**.
- 6 Specify the number of times a host is permitted to attempt to connect to a monitored service before being blocked in the **Trigger count before blocking** field. This option only takes effect when one of the blocking options is enabled. The trigger count value should be between 0 and 2 (zero represents an immediate blocking of probing hosts). Larger settings mean more attempts are permitted before blocking and although allowing the attacker more latitude; these settings reduce the number of false positives.
 - Default: 0
 - Range: 0-2
- 7 [Optional] Enter the IP addresses of trusted servers and hosts in the **Addresses to ignore for detection and block purposes** text box. The IDB ignores the list of host IP addresses. You can freely edit the list; however, you cannot remove the addresses *0.0.0.0* and *127.0.0.1* since they represent the IDB host. You can enter IP addresses as a range.
- 8 Click **Submit**.

Selecting TCP dummy services

Use this procedure to set the network ports scanned for TCP services. You can choose Basic, default Standard, or Strict settings, and add your own custom entries. To view a list of the services available for each setting, see Table 18 on page 288.

Prerequisite: Detect TCP probes must be enabled in the IDB configuration for activating scanning and blocking. See “Configuring basic IDB” on page 285.

- 1 From the **Firewall** menu, click **Intrusion Detection > TCP** tab. The TCP page appears.

Figure 216: IDB TCP tab

The screenshot shows the IDB configuration window with the TCP tab selected. The 'Network Ports scanned' list contains the following services: tcpmux, systat, netstat, finger, pop3, sunrpc, nntp, imap, uuwp, rlxbase, socks, and ingreslock. The 'Basic', 'Standard', and 'Strict' buttons are visible below the list. A 'Submit' button is at the bottom of the form. A note at the bottom of the form reads: 'Either manually edit the port list above, or initialize the list by pressing one of the predefined policy buttons.'

- 2 Select an option for the **Network Ports scanned** list:
 - **Basic:** Installs a minimal selection of ports to monitor while still providing sufficient coverage to detect many intruder scans.
 - **Standard (default):** Extends the Basic coverage by introducing additional monitored ports for early detection of intruder scans.
 - **Strict:** Installs a comprehensive selection of ports to monitor and should be sufficient to detect most scans. The Strict setting includes all services in Standard and Basic in addition to its own unique settings.



Security Alert: The list of network ports can be freely edited; however, adding network ports used by services running on the SnapGear unit (such as telnet) may compromise the security of the device and your network. It is strongly recommended to use only the predefined lists of network ports (Basic, Standard, Strict).

- 3 If you have changed the current configuration, a message informs you custom changes will be lost and prompts you to confirm your selection. Click **Apply** to accept.
- 4 Click **Submit**.

TCP network services

The predefined Basic, Standard, and Strict settings are listed in Table 18. An 'X' indicates the service is included in the setting; an em dash (—) indicates the service is not available in a setting.

Table 18: TCP services settings

Service	Basic	Standard	Strict
40421	—	X	X
40425	—	—	X
49724	—	X	X
bo2k	—	X	X
dc	—	—	X
discard	—	—	X
echo	—	—	X
Elite	—	X	X
exec	—	—	X
filenet-rmi	X	X	X
finger	—	X	X
gopher	—	—	X
http	—	—	X
ida-discover2	—	—	X
imap	X	X	X
ingreslock	X	X	X
ircd	—	X	X
italk	X	X	X
login	—	—	X
nburn_id	X	X	X
NetBus	X	X	X

Service	Basic	Standard	Strict
netstat	X	X	X
newoak	—	—	X
nntp	—	X	X
pop2	—	—	X
pop3	X	X	X
printer	—	—	X
rlzdbase	X	X	X
shell	—	—	X
sieve	X	X	X
socket23	—	—	X
socks	X	X	X
sometimes-rpc7	X	X	X
sometimes-rpc9	X	X	X
sometimes-rpc11	—	X	X
sunrpc	X	X	X
systat	X	X	X
tcpmux	X	X	X
terabase	—	—	X
uucp	X	X	X
x11	—	—	X
x11-1	—	—	X

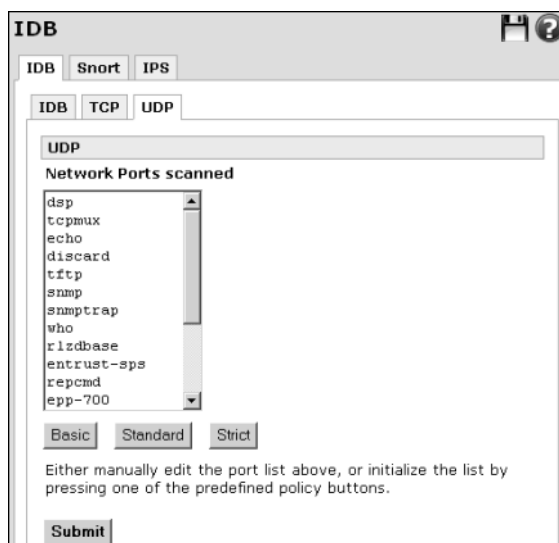
Selecting UDP dummy services

Use this procedure to set the network ports scanned for TCP services. You can choose Basic, default Standard, or Strict settings, and add your own custom entries. To view a list of the services available for each setting, see Table 18 on page 288.

Prerequisite: Detect UDP probes must be enabled in the IDB configuration for any scanning or blocking to occur. See “Configuring basic IDB” on page 285.

- 1 From the **Firewall** menu, click **Intrusion Detection > UDP** tab. The UDP page appears.

Figure 217: IDB UDP tab



- 2 Select an option for the **Network Ports scanned** list:
 - **Basic:** Installs a minimal selection of ports to monitor while still providing sufficient coverage to detect many intruder scans.
 - **Standard (default):** Extends the Basic coverage by introducing additional monitored ports for early detection of intruder scans. The Standard setting includes all of the Basic services.
 - **Strict:** Installs a comprehensive selection of ports to monitor and should be sufficient to detect most scans. The Strict setting includes all services in Standard and Basic in addition to its own unique settings.



Security Alert: The list of network ports can be freely edited; however, adding network ports used by services running on the SnapGear unit (such as telnet) may compromise the security of the device and your network. Secure Computing strongly recommends to use only the predefined lists of network ports (Basic, Standard, Strict).

- 3 If you have changed the current configuration, a message informs you custom changes will be lost and prompts you to confirm your selection. Click **Apply** to accept.
- 4 Click **Submit**.

UDP network services

The predefined Basic, Standard, and Strict settings are listed in Table 19. An 'X' indicates the service is included in the setting; an em dash (—) indicates the service is not available in a setting.

Table 19: UDP services settings

Service	Basic	Standard	Strict
BackOrifice	X	X	X
bo2k	X	X	X
discard	X	X	X
echo	X	X	X
entrust-sps	X	X	X
epp-700	X	X	X
filenet-nch	X	X	X
filenet-rmi	X	X	X
mdqs	—	—	X
mpm-flags	—	—	X
nfs	—	—	X
ntalk	—	—	X
repcmd	—	X	X
rlzdbase	—	X	X
snmp	X	X	X
snmptrap	X	X	X
sometimes-rpc10	X	X	X
sometimes-rpc12	X	X	X
sometimes-rpc8	X	X	X
ssh	X	X	X
sql*net	—	—	X

Service	Basic	Standard	Strict
sunrpc	—	—	X
talk	—	—	X
tcpmux	X	X	X
tftp	X	X	X
who	X	X	X

Advanced Intrusion Detection and Prevention

Note: The SG565, SG580, SG640, and SG720 models provide Advanced Intrusion Detection and Blocking in addition to basic IDB.

Advanced Intrusion Detection and Prevention is based on two variants of the tried and tested intrusion detection and prevention system Snort v2. Snort in IDS (Intrusion Detection System) mode resides in front of the firewall, and detects and logs a very wide range of attacks. Snort in IPS (Intrusion Prevention System) mode resides behind the firewall, and detects and blocks a wide range of attacks.

The primary advantage of running Snort IDS (Snort) in front of the firewall is that it sees unfiltered network traffic, and is therefore able to detect a wider range of attacks. The primary advantage of running Snort IPS (IPS) behind the firewall is that suspicious network traffic can be disallowed rather than simply being flagged as suspicious and allowed to pass.

Snort uses a combination of methods to perform extensive ad hoc network traffic analysis. These include protocol analysis, inconsistency detection, historical analysis, and rule-based inspection engines. Snort can detect many attacks by checking destination port number, TCP flags, and doing a simple search through the packet's data payload. Rules can be quite complex; allowing a trigger if one criterion matches but another fails and so forth. Snort can also detect malformed network packets and protocol anomalies.

Snort can detect attacks and probes such as buffer overflows, stealth port scans, CGI attacks, NetBIOS SMB probes, OS finger printing attempts, and many other common and uncommon exploits.

You can use Snort in IDS and IPS mode simultaneously if you choose; however, it consumes much of the memory on the SnapGear appliance. If you run both modes, make sure you enable the user less memory feature in the IPS configuration. See "Configuring Snort in IPS mode" on page 293.

About rule sets

The snort detection uses rule sets that can be individually enabled or disabled. Rule sets are sets of defined patterns or rules used for the detection of attacks. These are grouped by type such as ddos, exploit, backdoor, and netbios. Each group encompasses many attack signatures. The full list of signatures can be viewed at the Snort Web site (<http://www.snort.org>).

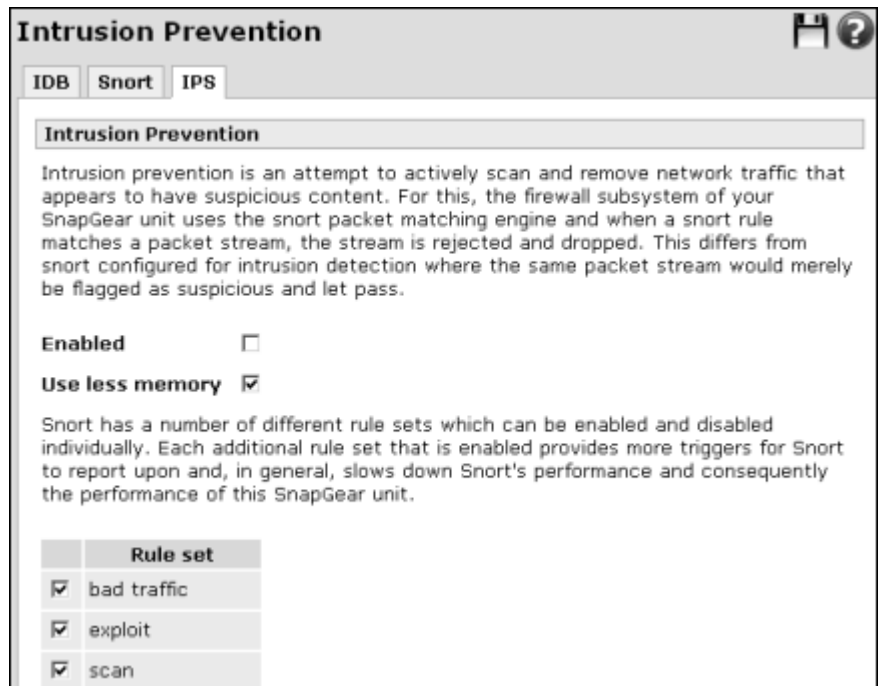
The more rule sets selected, the greater the load imposed on the appliance. Therefore, a conservative rather than aggressive approach to adding rule sets should be followed initially.

Configuring Snort in IPS mode

Use this procedure to configure IPS.

- 1 From the **Firewall** menu, click **Intrusion Detection > IPS** tab. The Intrusion Prevention page appears.

Figure 218: Snort Configuration-IPS



The screenshot shows the 'Intrusion Prevention' configuration window. At the top, there are three tabs: 'IDB', 'Snort', and 'IPS', with 'IPS' being the active tab. Below the tabs is a section titled 'Intrusion Prevention' containing a descriptive paragraph about intrusion prevention. Underneath this, there are two settings: 'Enabled' with an unchecked checkbox and 'Use less memory' with a checked checkbox. A paragraph explains that enabling more rule sets slows down performance. At the bottom, there is a table with the heading 'Rule set' containing three rows: 'bad traffic', 'exploit', and 'scan', each with a checked checkbox in the first column.

	Rule set
<input checked="" type="checkbox"/>	bad traffic
<input checked="" type="checkbox"/>	exploit
<input checked="" type="checkbox"/>	scan

- 2 Select the **Enabled** check box.

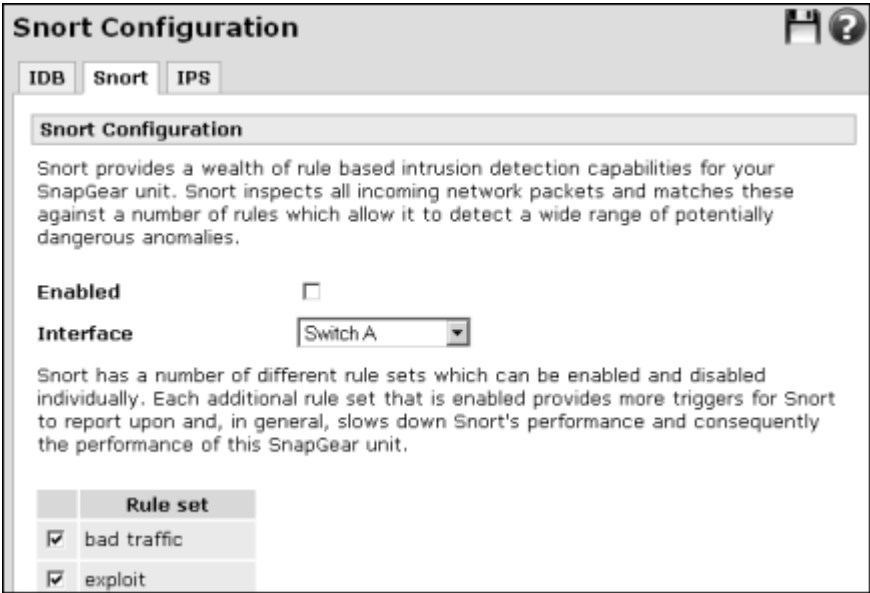
- 3 [Recommended] To restrict memory usage for the scanning, select the **Use less memory** check box. This results in slower signature detection throughput, but may be necessary if the appliance is configured to run many services, many VPN tunnels, or both Snort IDS and IPS.
- 4 Select the check box or check boxes for the **Rule sets** you want to enable for snort detection. All rules sets are selected by default.
- 5 Click **Submit**.

Configuring Snort in IDS mode

Use this procedure to configure snort detection in IDS mode.

- 1 From the **Firewall** menu, click **Intrusion Detection > Snort** tab. The Snort Configuration page appears.

Figure 219: Snort Configuration page



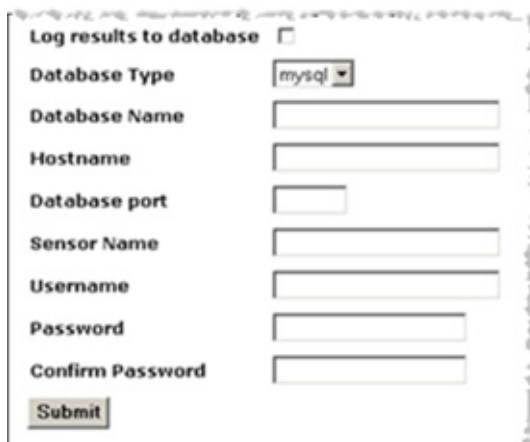
- 2 Select the **Enabled** check box.
- 3 Select the network **Interface** to monitor. This is typically **Internet**, or possibly **DMZ**.
- 4 Select the check box or check boxes for the **Rule sets** you want to enable for snort detection. All rule sets are enabled by default.
- 5 Click **Submit**. You can also log results of the snort detection to a MySQL database rather than the syslog. For more information, see "Logging to an analysis server (Snort IDS only)".

Logging to an analysis server (Snort IDS only)

Typically, Snort in IDS mode is configured to log intrusion attempts to a remote database server, which in turn runs an analysis console. An analysis console, such as BASE (Basic Analysis and Security Engine), is an application purpose-built for analyzing this log output. See “Setting up the analysis server for Snort IDS” on page 296 for information about analysis server tools.

- 1 From the **Firewall** menu, click **Intrusion Detection > Snort** tab. The Snort Configuration page appears. Scroll to the bottom of the page to the log results area.

Figure 220: Log IDS to MySQL DB



The screenshot shows a web form titled "Log results to database" with a checkbox. Below it are several input fields: "Database Type" (a dropdown menu showing "mysql"), "Database Name", "Hostname", "Database port", "Sensor Name", "Username", "Password", and "Confirm Password". A "Submit" button is at the bottom.

- 2 [Optional] To log to a MySQL database, select the **Log results to database** check box. If the check box is cleared, results are output to the system log.
- 3 The device currently supports only the **MySQL Database Type**.
- 4 Enter the table name of the remote database in the **Database Name** field.
- 5 Enter the IP address or resolvable host name of the analysis server in the **Hostname** field.
- 6 Enter the database port of the analysis server in the **Database port** field. For MySQL type databases, this is typically 3306.
- 7 [Optional] To prepend an arbitrary string to the log output, enter the string in the **Sensor Name** field. This may be useful if you have deployed more than one intrusion detection system and need to differentiate analysis between them.
- 8 Enter the user name and password required for authentication to the remote database in the **User name** and **Password** fields. Repeat the password in the **Confirm Password** field.
- 9 Click **Submit**.

Setting up the analysis server for Snort IDS

Specific open source tools are required to be installed on the analysis server for a straightforward evaluation. The analysis server is typically a Pentium 4-level system running Linux (such as Red Hat and Debian) with sufficient memory and disk capacity to run a database and Web server with at least one ethernet port. With these tools installed, Web pages can be created that display, analyze, and graph data stored in the MySQL database from the SnapGear appliance running Advanced Intrusion Detection. They should be installed in the following order:

1 MySQL database

<http://www.mysql.com/downloads/mysql-4.0.html>

<http://www.mysql.com/doc/en/index.html>

2 Apache Web server

<http://httpd.apache.org/download.cgi>

<http://httpd.apache.org/docs-2.0/>

3 PHP scripting language for developing Web pages

<http://www.php.net/downloads.php>

<http://www.php.net/download-docs.php>

4 ADODB library to hide differences between databases used by PHP

<http://php.weblogs.com/adodb#downloads>

5 GD graphics library for GIF image creation used by PHP

<http://www.boutell.com/gd/>

6 PHPlot graph library for charts written in PHP

<http://www.phplot.com/>

7 BASE analysis console

<http://secureideas.sourceforge.net/>

Snort is running as an IDS sensor on the SnapGear appliance, logging to the MySQL database on the analysis server. The Downloads section of the BASE Web site contains detailed documents that aid in installing the above tools on the analysis server.

Access control

Access control minimizes inappropriate Internet use. The access control Web proxy allows you to control access to the Internet based on the type of Web content being accessed (Webwasher), and which user or workstation is accessing the Internet content (Require user authentication, IP Lists). Additionally, you can set up global block and allow lists for Web sites you always want to be accessible or inaccessible (Web Lists), and ensure they are not running network services that may be exploited (Policy) before accessing the Internet.

Access control options operate in the following order for Web (HTTP protocol only) access:

- 1 Web Lists allow
- 2 Web Lists deny
- 3 Security Policy enforcement
- 4 ACL allow lists
- 5 ACL block lists
- 6 Username/password (if Bypass Content Filtering is set for a specified user)
- 7 Content filtering (Webwasher)

Access control options operate in the following order for all other Internet (non-HTTP protocols) access:

- 1 Security Policy enforcement
- 2 ACL allow lists
- 3 ACL block lists

For more detail on how access controls interact with other firewall features such as packet filtering and IPS, see “Controlling packet traffic” on page 202.

Authorizations page

Use this page to limit which users have access to the Internet through the appliance.

Figure 221 shows the access control main authorizations page:

Figure 221:
Authorizations setup —
Main tab

The screenshot shows the 'Authorizations' configuration page with the 'Main' tab selected. The page title is 'Authorizations' with a save icon and a help icon. Below the title are tabs for 'Main', 'ACL', 'Web Lists', 'Policy', and 'Webwasher'. The 'Authorization setup' section includes a header 'Enable Access Control' followed by four buttons: 'Private', 'Internet', 'DMZ', and 'Guest'. The 'Internet' button is checked. Below these are settings for 'Require User Authentication' (unchecked), 'Default Action' (set to 'Allow'), 'Syslog Level' (set to '0'), 'Fast Web Mode' (checked), and 'Web Proxy Port' (set to '81'). A 'Submit' button is at the bottom.

Private	Internet	DMZ	Guest
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Require User Authentication ☐

Default Action Allow ▾

Syslog Level 0

Fast Web Mode ☒

Web Proxy Port 81

Submit

Enabling access control

Use this procedure to enable access control. Access control must be enabled in order to use ACL, Webwasher, and other access control mechanisms available within the Access Control menu option.

- 1 From the **Firewall** menu, click **Access Control > Main** tab. The Authorizations setup page appears.

- 2 In the **Enable Access Control** pane, select the check box or boxes for the firewall classes to which you want to apply access control. At least one check box must be selected for any access control operation to take place. Available options are:
 - **Private** (includes the LAN, VPN, and Dialin firewall classes)—Enables access controls on traffic destined to the private network.
 - **Internet**—[Recommended] Enables traffic destined to devices on the Internet.
 - **DMZ**—Enables traffic destined to the DMZ.
 - **Guest**—Enables traffic destined to the Guest network.
- 3 [Optional] To require users to authenticate for access to the Web through the SnapGear appliance, select the **Require User Authentication** check box. This check box must be selected to view Webwasher filtering reports on an individual user basis. For more information, see “Enabling Webwasher content filtering” on page 319. The browser must also be configured. See “Configuring browsers to use the appliance Web proxy” on page 302.

Access control users should generally have only the **Internet Access (via Access Controls)** check box selected, with all other access permissions cleared. For information on setting up users, see “Adding a local user” on page 480.
- 4 The **Default Action** list defines the behavior when none of the access control settings definitively allow or block access. Available options are:
 - **Allow** (default, recommended)
 - **Block**—If selected, allow access must be explicitly enabled elsewhere in access control (for instance, Web Lists URL Allow; or for ACL Black and White lists, indicate Allowed Source and Destination Hosts) to allow some network traffic or no access is possible. The fixed order of access control rule evaluation is not adjusted as a result of using the default block action, which must be carefully taken into consideration when configuring access controls.
- 5 The **Syslog Level** controls the level of debug output to the system log. The higher the value, the more verbose the output. For normal operation, this should be set to **0** since very large logs and a noticeable system slowdown might result. For normal debugging, set to **1**. Higher levels need only be turned on when directed to by Secure Computing technical support.
 - Default: 0
 - Range: 0-5

Tip: if you need to increase the debugging level, you also need to either increase the local syslog buffer size, or have remote logging enabled. See “Configuring local system log settings” on page 499 and “Enabling remote system logging” on page 501.

- 6 [Optional] To bypass the relatively slow software HTTP proxy under certain conditions, select the **Fast Web Mode** check box. This results in faster Web accesses by trading away the informative error pages when sites are blocked. The conditions required for possible bypass are:
 - There are no allow or deny Web lists defined.
 - Webwasher content filtering is not enabled.
 - Web antivirus is not enabled.
- 7 The **Web Proxy Port** controls the TCP port number that the access control HTTP proxy listens on. Typically you do not need to change this number unless you want to run another service on the SnapGear appliance at this port number.
 - Default: 81
 - Range: 1-65535

Note: *HTTPS (Secure Web) proxy access control mechanisms are not currently supported, other than those provided for all other non-HTTP protocols.*

- 8 Click **Submit**.

Disabling access control

- 1 From the **Firewall** menu, click **Access Control > Main** tab. The Authorizations setup page appears.
- 2 Clear all of the **Enable Access Control** check boxes.
- 3 Click **Submit**.

User authentication for Internet access

When a user attempts to access a Web site on the Internet, the browser displays a dialog box similar to the following:

Figure 222: Access control log in



Users without Web proxy access see a screen similar to the figure below when attempting to access external Web content:

Figure 223: No Web proxy access

User Authentication

You must enter a valid Username and Password to authenticate against the access control lists to access the Internet. Your user account must also have Web access enabled by your administrator. Without this your access will be blocked.

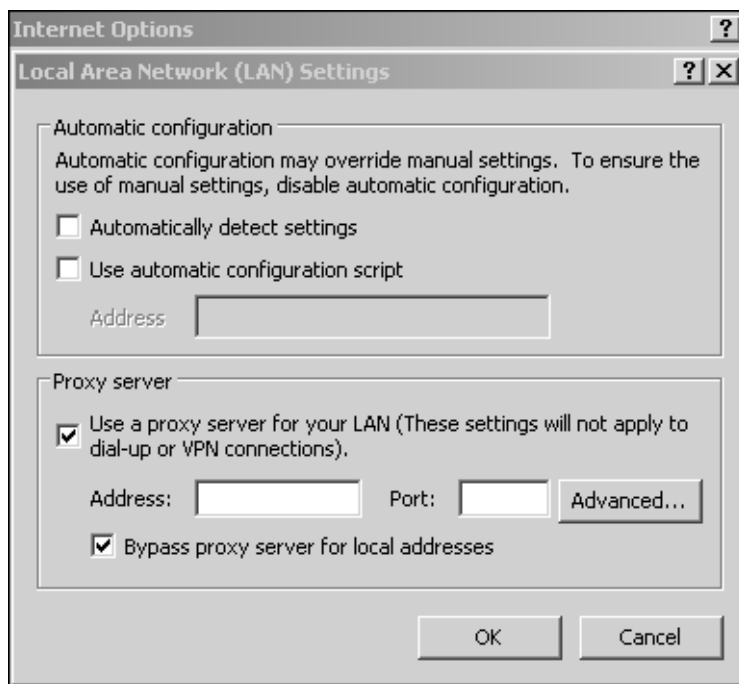
If your users see the message “You must enter a valid Username and Password to authenticate access control lists to access the Internet. Your user account must also have Web access enabled by your administrator. Without this your access will be blocked” as shown in Figure 223, then configure the browser to use the appliance Web proxy. See “Configuring browsers to use the appliance Web proxy” on page 302.

Configuring browsers to use the appliance Web proxy

In order for user-based access controls to prompt for login and password, each browser on the LAN must be configured to use the Web proxy of the SnapGear appliance. The example given is for Microsoft Internet Explorer 6. Instructions for other browsers should be similar; refer to their documentation for details on using a Web proxy.

- 1 From the **Internet Options** menu, click **Tools > Connections** tab. Click **LAN Settings**.

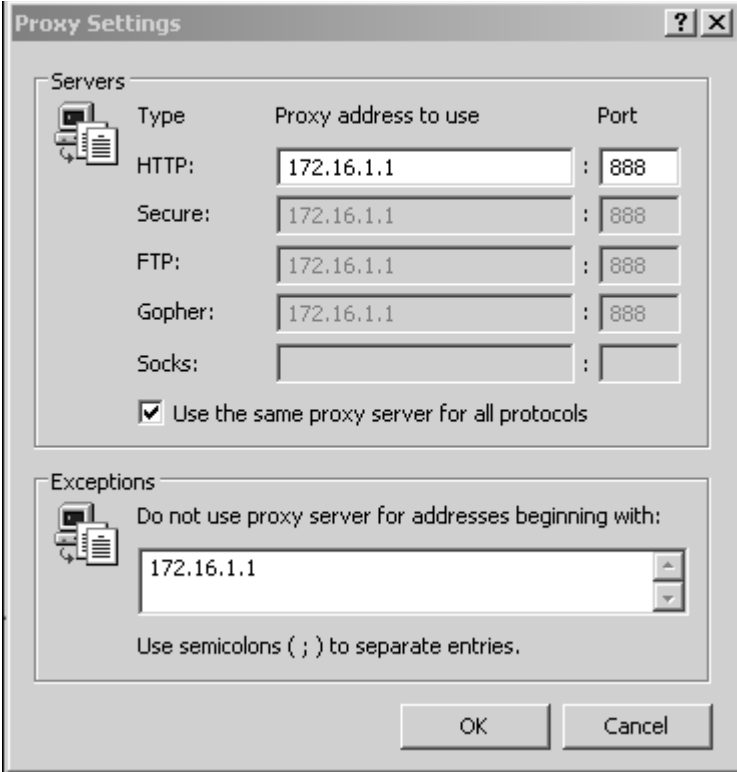
Figure 224: Local Area Network (LAN) Settings for user access control



- 2 Select the **Use a proxy server for your LAN...** and the **Bypass proxy server for local addresses** check boxes. All other options should remain cleared.
- 3 Click **Advanced**.

The Proxy Settings dialog box is displayed.

Figure 225: Local Area Network (LAN) Settings for user access control



The Proxy Settings dialog box is shown with the following configuration:

Type	Proxy address to use	Port
HTTP:	172.16.1.1	888
Secure:	172.16.1.1	888
FTP:	172.16.1.1	888
Gopher:	172.16.1.1	888
Socks:		

☒ Use the same proxy server for all protocols

Exceptions

Do not use proxy server for addresses beginning with:

172.16.1.1

Use semicolons (;) to separate entries.

OK Cancel

- 4 In the row labeled **HTTP**, enter the LAN IP address of the appliance in the **Proxy address to use** column, and your Web server port in the **Port** column. Leave the other rows blank. For information on setting the Web server port, see “Web Management Configuration page” on page 208.
- 5 In the **Exceptions** text box, enter the LAN IP address of the appliance.
- 6 Click **OK** in each subsequent dialog box until done.

ACL tab

The ACL (Access Control Lists) enables configuration of allowed and blocked source and destination hosts using addresses defined on the Addresses page. Access can be blocked or allowed by the source (LAN) IP address or address range, the Destination (Internet) host's IP address or address range, or the Destination Host's name. The source/destination address of the current network request will be matched against the list of firewall groups, IP addresses, IP address ranges and host IP address. A successful match allows or blocks the network request as appropriate. There is no performance hit for increasing the size of an IP address range and negligible cost for increasing the number of ranges, groups, or hosts.

Note: All Internet traffic, not just Web traffic, is affected by ACL.

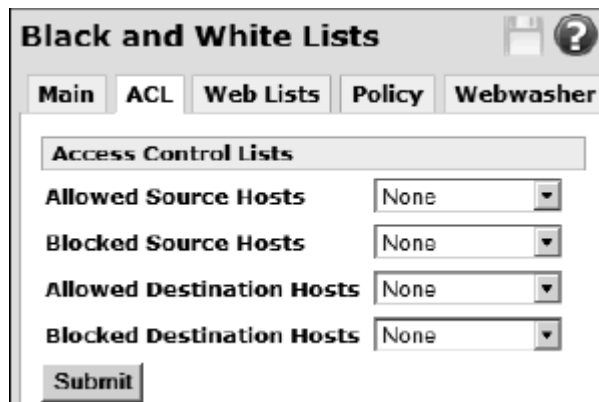
Prerequisites:

- ACLs require previously configured Definitions to allow or deny. Addresses are added through the Definitions menu. Refer to the “Definitions” on page 219 for further details.
- Access control must be enabled. See “Enabling access control” on page 298.

Configuring ACL

- 1 From the **Firewall** menu, click **Access control > ACL** tab. The Access Control (Black and White) Lists page appears.

Figure 226:
ACL



- 2 [Optional] Select allowed source hosts from the **Allowed Source Hosts** list. The default is None. Available options depend upon the Addresses defined in the Definitions menu.

- 3 [Optional] Select blocked source hosts from the **Blocked Source Hosts** list. The default is None. Available options depend upon the Addresses defined in the Definitions menu.
- 4 [Optional] Select allowed destination hosts from the **Allowed Destination Hosts** list. The default is None. Available options depend upon the Addresses defined in the Definitions menu.
- 5 [Optional] Select blocked destination hosts from the **Blocked Destination Hosts** list. The default is None. Available options depend upon the Addresses defined in the Definitions menu.
- 6 Click **Submit**.

Example ACL: Blocked and allowed hosts

This example defines block rules that stop a range of addresses, with an allow rule that exists as an exception to the block rules. Since the allow is checked before the block, you can grant access to override the block rule.

In this scenario, the LAN has an address of 10.0.0.0/24. All source hosts allowed access to the LAN are number 128 and above, and all source hosts below that range are not allowed access. A block rule for the range 0-127 prevents access to those source hosts. However, there is an exception to this policy in that a source host with address 10.0.0.15 requires access. An allow rule can grant access in this circumstance.

- 1 From the **Firewall** menu, click **Definitions > Addresses** tab. The Addresses page appears.
- 2 Select **Single Address or Range** and click **New**.
- 3 Enter **10 . 0 . 0 . 0 - 127** as the range of addresses to block in the **IP Address** field and click **Finish**. Notice the field automatically converted converted the address range from 10.0.0.0-127 to 10.0.0.0/25. The latter CIDR format (Classless Inter-Domain Routing) is a simpler format for the network stack and rules to understand and also the more modern way of expressing ranges that end nicely on 2ⁿ boundaries, so the SnapGear Web console recognizes them and performs a conversion automatically where appropriate.
- 4 Enter **10 . 0 . 0 . 15** as the single address to allow in the **IP Address** field and click **Finish**.
- 5 From the **Firewall** menu, click **Access control > ACL** tab. The Access Control (Black and White) Lists page appears.
- 6 In the **Allowed Source Hosts** list, select the single address you defined, which is **10 . 0 . 0 . 15**. You can also provide a name for the address, but this example just uses the IP addresses without names.
- 7 In the **Blocked Source Hosts** list, select the single address you defined, which is **10 . 0 . 0 . 0 / 25**.
- 8 Click **Submit**.

Figure 227:
ACL example

Black and White Lists

Main ACL Web Lists Policy Webwasher

Access Control Lists

Allowed Source Hosts 10.0.0.15

Blocked Source Hosts 10.0.0.0/25

Allowed Destination Hosts None

Blocked Destination Hosts None

Submit

Web Lists tab

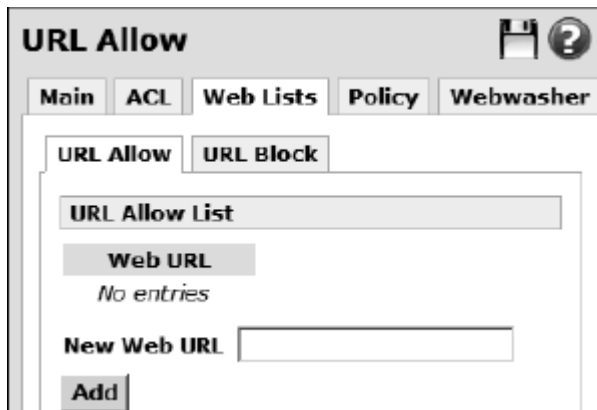
Use the tabs within Web Lists to configure allowed and blocked URL fragments. Only WWW browsing is restricted by these settings. If a requested URL matches contains any of the defined URL fragments defined, the rule is triggered. You can grant or deny access to any Web address (URL) that contains text or a complete URL defined under the URL Block or Allow lists. Entering xxx blocks access to any URL containing xxx; for example, all of the following URLs are blocked: <http://www.xxx.com>, <http://xxx.example.com>, or www.test.com/xxx/index.html.

Tip: Defining overly short URL fragments can result in many sites matching and being allowed or denied erroneously. For better accuracy, define complete URLs. However, hundreds or even thousands of reasonable length fragments can be defined and incur only a slight time cost for filtering.

Adding an allowed URL

- 1 From the **Firewall** menu, click **Access control > Web Lists** tab > **URL Allow** tab. The URL Allow List page appears.

Figure 228: URL Allow
tab



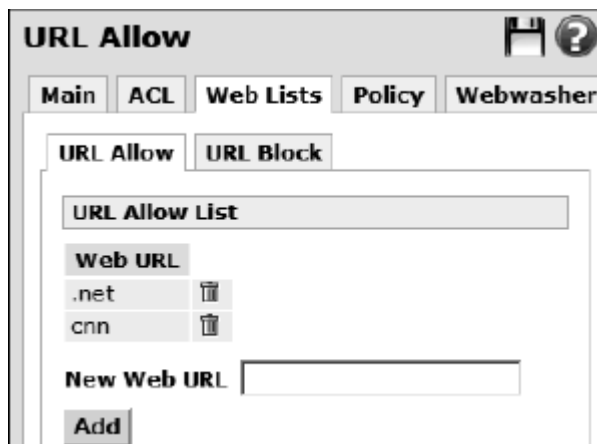
- 2 Enter a complete URL or a character string in the **New Web URL** field.
 - Maximum characters: 500
- 3 Click **Add**. The URL is added to the Web URL list of allowed URLs. Repeat as necessary.

Deleting an allowed URL or URL fragment

Use this procedure to delete an allowed URL or URL fragment.

- 1 From the **Firewall** menu, click **Access control > Web Lists tab > URL Allow** tab. The URL Allow List page appears.

Figure 229: URL Allow
List



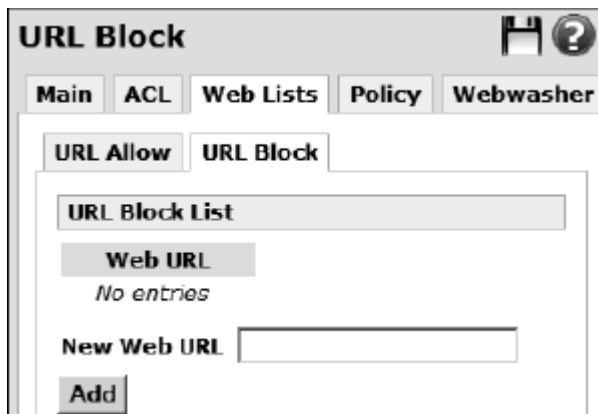
- 2 Click the delete icon for the URL or fragment you want to delete. An action successful message is displayed.

Blocking a URL

- 1 From the **Firewall** menu, click **Access control > Web Lists tab > URL**

Block tab. The URL Block List page appears.

Figure 230: URL Block



The screenshot shows a window titled "URL Block" with a toolbar containing a save icon and a help icon. Below the title bar are five tabs: "Main", "ACL", "Web Lists", "Policy", and "Webwasher". The "Web Lists" tab is selected, and within it, the "URL Block" sub-tab is active. The main area displays a "URL Block List" section with a "Web URL" label and the text "No entries". Below this is a "New Web URL" label followed by a text input field. At the bottom left of the input area is an "Add" button.

- 2 Enter the URL or fragment in the **New Web URL** field.
- 3 Click **Add**. The URL is added to the Web URL list of blocked URLs. Repeat as necessary.

Deleting a blocked Web URL

Use this procedure to delete or unblock a blocked URL.

- 1 From the **Firewall** menu, click **Access control > Web Lists tab > URL Block** tab. The URL Block List page appears.
- 2 Click the delete icon for the URL you want to unblock. An action successful message is displayed. The URL is allowed access again.

Policy enforcement

Policy enforcement on the SnapGear appliance provides the ability for specific internal servers and workstations to have their network access through the appliance denied based on the results of probes performed periodically by the appliance. The built-in functionality allows network access to be denied, including internet and VPN access, based on the TCP services a server or workstation is running.

The SG565, SG580, SG640, and SG720 models have the ability to enforce a security policy based on the results of a NASL (Nessus Attack Scripting Language) script. NASL is the scripting language similar to the C programming language used by the Nessus vulnerability network scanner to perform its vulnerability tests. To download NASL scripts, go to the following URL: <http://cgi.nessus.org/plugins/>. You can also write your own scripts. A NASL reference guide is available at the following URL: <http://www.virtualblueness.net/nasl.html>.

This section contains the following topics:

- “Enabling security policy enforcement” on page 311
- “Creating a security policy group” on page 313
- “Uploading a NASL script” on page 316
- “Managing policy enforcement scripts” on page 315

Enabling security policy enforcement

This access control module allows a site's security policy to be partially actively enforced. Hosts that do not adhere to their defined policy are automatically denied access through the firewall. A number of security groups can be defined where each group contains a number of host IP addresses or IP address ranges. For further information, see “Creating a security policy group” on page 313. Each group is additionally given a number of permitted and denied services that they are allowed to offer. Each host in each group are periodically actively scanned for the services they are not allowed to offer and if a connection to one of these services is successful, the host is blacklisted until such time as the offending service is no longer offered. Scans are never performed against permitted services.

A number of predefined allow and deny service lists are provided; however, these should be considered a guideline only, as they are not a replacement for a well-designed security policy.

To enable and configure security policy enforcement

- 1 From the **Firewall** menu, click **Access Control > Policy** tab. The Policy Enforcement page appears.

Figure 231: Policy Enforcement page

Policy Enforcement

Main ACL Web Lists **Policy** Webwasher

Policy Script Management Script Upload

Security Policy Enforcement

Enable Policy Enforcement ☐

Block Unscanned Hosts ☐

Simultaneous Probes

Minimum Inter Probe Delay (seconds)

Submit

Security Group	Description
No entries	

New

- 2 To enable policy enforcement, select the **Enable Policy Enforcement** check box. Turning policy enforcement on without specifying anything to scan causes a slight decrease in performance of the appliance.
- 3 [Optional] Select the **Block Unscanned Hosts** check box. This check box specifies the behavior taken when a host scheduled to be scanned but not actually been scanned yet attempts to access the Internet. By default, the host would be allowed access. By checking this box, the host would be denied access instead.

- 4 Enter the maximum number of different hosts to scan together in the **Simultaneous Probes** field. This specifies the maximum number of simultaneous scanning processes allowed to exist at any single point in time. Specifying a larger number reduces the time a security scan takes, but increases the load of doing so both on the network and on the appliance. Specifying too large a number could result in the appliance exhausting its memory and the scan failing completely.
 - Default: 4
 - Integer value equal to or greater than 1
- 5 Enter the minimum number of seconds between scans of a single host in the **Minimum Inter Probe Delay** field. The delay specifies the minimum interval between starting successive security scans. If a scan takes longer than the specified number of seconds to complete, the setting is ignored and scanning is continuous. However, if a scan takes less time to perform than this setting, the following scan is delayed until this number of seconds has elapsed since the start of the current scan. This setting also determines the maximum time for changes to take effect.
 - Integer value equal to or greater than 1
 - Default: 1800
- 6 Click **Submit**.

Disabling security policy enforcement

- 1 From the **Firewall** menu, click **Access Control > Policy** tab. The Policy Enforcement page appears.
- 2 Clear the **Enable Policy Enforcement** check box.
- 3 Click **Submit**.

Creating a security policy group

Use this procedure to create a security policy enforcement groups. A selection of different hosts can be defined along with allowed and disallowed services. The security policy enforcement feature of access control periodically scans for policy adherence.

The actual definition of these policy groups is very flexible. In particular, hosts are allowed to be present in multiple security policy groups. If this is the case, an allowed service in any of the groups overrides a denied service in all the other groups to which the host belongs. Also, if additional security scripts are specified, then all such scripts will be run against the target host once each and any single failure denies access.

Prerequisites:

- Define addresses and services groups. See “Addresses page” on page 223 and “Creating a service group” on page 221.
- Enable policy enforcement. See “Enabling security policy enforcement” on page 311.
- Upload and test NSAL scripts (optional). See “Uploading a NASL script” on page 316 and “Managing policy enforcement scripts” on page 315.

To create a security policy group

- 1 From the **Firewall** menu, click **Access Control > Policy** tab. The Policy Enforcement page appears.
- 2 To configure a Security Group, click **New**. The Modify Security Policy Group page appears.

Figure 232: Policy tab —
Modify Security Policy
Group

Policy Enforcement

Main ACL Web Lists **Policy** Webwasher

Policy Script Management Script Upload

Modify Security Policy Group

Name: NASL

Description: test

Scanned Host(s): RFC1918 A

Allowed Service(s): HTTP (Web)

Blocked Service(s): Telnet

NASL Scripts

☐ finger.nasl





Finish Cancel

- 3 Enter a name for the policy group in the **Name** field. The Name field must be unique across all security policy groups. The name can be 1 or more characters of any type.
- 4 [Optional] Enter a description in the **Description** field.
- 5 Select the host from the **Scanned Host** list. The entries available in the list are defined in the Addresses page. For information, see “Addresses page” on page 223.
- 6 [Optional] Select a service group from the **Allowed Services** list. The service group specifies the services which the hosts in this group are allowed to run. These services are not scanned for during the security policy scans of the included hosts. The entries available in the list are defined in the Service Groups page. For information, see “Service Groups page” on page 220.
- 7 [Optional] Select a service to block from the **Blocked Services** list.
- 8 Click **Submit**.

Editing a security policy group

- 1 From the **Firewall** menu, click **Access Control > Policy** tab. The Policy Enforcement page appears.
- 2 In the Security Group pane, click the edit icon for the security group you want to edit.

Figure 233: Defined Security Groups

Security Group	Description		
NASL	test		
Finger			

- 3 The Modify Security Policy Group page appears. Make your changes and click **Finish**.

Deleting a security policy group

- 1 From the **Firewall** menu, click **Access Control > Policy** tab. The Policy Enforcement page appears.
- 2 In the Security Group pane, click the delete icon for the security group you want to delete.

Managing policy enforcement scripts

In addition to enforcing the services aspect of security groups, it is possible to include a number of NASL scripts in the `/etc/config` directory on the appliance and to define some or all of these to be run against the target hosts. Typically, one would use attack scripts from the Nessus suite to scan for specific vulnerabilities and exploits on a host. If any script detects such vulnerability, Internet access is again blocked. The list of available scripts is automatically populated from the files ending with `.nasl` in the `/etc/config` directory.

Security groups may overlap with respect to hosts within them. In this case, a single allow service overrides any number of denies of that same service.



Caution: NASL scripts and overlapping groups do not interoperate particularly well and should be avoided.

Use the Script Management tab for management and testing of installed NASL scripts. By default, newly uploaded scripts appear but are available for use with a policy enforcement group until it is either manually enabled or fully validated.

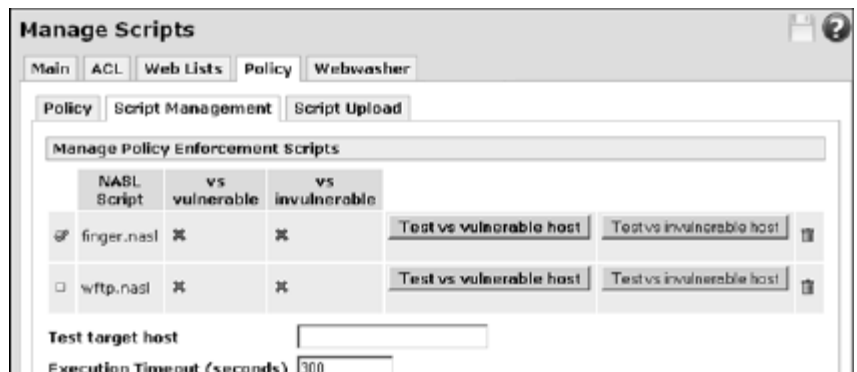
Prerequisites:

- Enable and configure policy enforcement. See “Enabling security policy enforcement” on page 311.
- Create policy security groups for your organization. See “Creating a security policy group” on page 313.
- Upload the NASL scripts you want to test. See “Uploading a NASL script” on page 316.

Testing an uploaded NASL script

- 1 From the **Firewall** menu, click **Access Control > Script Management** tab. The Manage Scripts page appears.

Figure 234: Script Management tab



To validate a script for use within policy enforcement it is advisable to execute the script against both a host vulnerable to and a host invulnerable to the security vulnerability for which you are checking. The table of scripts provides two testing buttons for this purpose. The table also contains two check boxes indicating if the two tests have been successfully executed for each script.

- 2 In the **Test target host** field, enter the host you intend to test the selected NASL script against. Specify the host as either a hostname or an IP address.
- 3 In the **Execution Timeout (seconds)** field, enter how long before ending the test if a concrete result is not returned in that timeframe. Typically, the default setting of 300 seconds does not require adjustment.
- 4 Select the appropriate Test button: **Test vs vulnerable host** or **Test vs Invulnerable host**. A message indicates testing of the script is underway. Results of the test are recorded in the Syslog. Be sure to run the test against both vulnerable and invulnerable hosts. Once you successfully test against vulnerable and invulnerable hosts, the script is deemed safe to use. In the **vs.** columns, crossmarks indicate an unsuccessful test; checkmarks indicate a successful test.

Disabling a policy enforcement script

- 1 From the **Firewall** menu, click **Access Control > Script Management** tab. The Manage Scripts page appears.
- 2 Click the enabled check box to disable the script. The check mark no longer displays, indicating the script is now disabled.

Deleting a policy enforcement script

- 1 From the **Firewall** menu, click **Access Control > Script Management** tab. The Manage Scripts page appears.
- 2 Click the delete icon for the script you want to delete. An action successful message is displayed.

Uploading a NASL script

Use this procedure to upload NASL scripts to the appliance. NASL is the part of the Nessus vulnerability scanner that performs the majority of the vulnerability checks.

- 1 From the **Firewall** menu, click **Access Control > Script Upload** tab. The Upload Scripts page appears.

Figure 235: Script Upload
Policy tab

Upload Scripts

Main ACL Web Lists Policy Webwasher

Policy Script Management Script Upload

Upload Policy Enforcement Scripts

Upload NASL script Browse...

Add

- 2 In the **Upload NASL script** field, either enter the file name or click **Browse** to locate the script file you want to upload.
- 3 Click **Add**. This file is uploaded to the SnapGear appliance and made available in the “Managing policy enforcement scripts” on page 315, where you must enable and validate the script.

Webwasher content filter service

Webwasher is the next generation of content filtering offered by Secure Computing. All new content filtering subscriptions are for the Webwasher service. You can purchase Webwasher URL filtering as an add-on feature, with or without the reporting option. After the purchase, you receive a certificate and private key to upload into the SnapGear appliance. The certificate identifies the appliance to the Webwasher servers and must be unique to each appliance. For information on activating add on features, see “Activating a feature” on page 16. For complete details on adding filter licenses according to your firmware version, refer to article **#2810** in the SnapGear knowledgebase portal:

<http://sgkb.securecomputing.com>

The Webwasher URL filter service on the SnapGear appliance is for the URL filtering (and reporting if applicable) feature only. Advanced Webwasher features include anti-malware, anti-virus, anti-spam, SSL scanner, and IM and peer-to-peer security. If you or your organization want to use the advanced features of Webwasher, you need to purchase a standalone Webwasher appliance to use in conjunction with the SnapGear appliance. For more information about Webwasher, visit the following URL:

<http://www.securecomputing.com/index.cfm?skey=22>

How Webwasher works with SnapGear

There are several Webwasher servers installed around the world, dedicated to providing URL filtering services to the SnapGear appliances, record activity and forward it to a reporting server if a reporting license has been purchased. The SnapGear appliance connects to the closest server based on IP addresses mapped to a geographic region.

When a user makes a request to access a URL on the Web, the request is routed to the SnapGear appliance. The appliance sends the URL request on to the Webwasher service. The Webwasher services returns a categorization for the requested URL to the appliance. The appliance compares the categorization to the blocked and allowed categories configured on itself and then acts accordingly. If the category is allowed, the user can view the URL they requested. If not, the user receives a message that their request failed validation. The appliance can cache category information for URLs to improve performance and avoid excessive traffic to the Webwasher service.

The basic steps for configuring and using Webwasher URL filter service are outlined below:

- 1 Enable and configure an NTP server to keep accurate time for certificate validity, reporting, and system logging. See “Enabling the NTP time server” on page 465.
- 2 Enter your certificate and private key for your Webwasher service into the SnapGear appliance with the method of your choice. See “Uploading a Webwasher certificate and key” on page 321 or “Copying and pasting a Webwasher certificate and key” on page 322.
- 3 Enable and configure Webwasher content filtering. See “Enabling Webwasher content filtering” on page 319.
- 4 Select the categories you want to block. See “Blocking categories for Webwasher filtering” on page 323.
- 5 View the reports of the URL filtering in action if your license includes reporting. See “Viewing Webwasher reports” on page 324.

Enabling Webwasher content filtering

Use this procedure to enable and configure Webwasher content filtering. The SnapGear appliance dynamically retrieves rating categories from the Webwasher server. As such, new categories might be added after content filtering is configured on your appliance.

Note: Content filtering is not performed for addresses specified in the **Web Lists** tab > **URL Allow or Block** pages or for allowed or blocked hosts specified in the **ACL** page. See “Web Lists tab” on page 307 and “ACL tab” on page 304 for further details.

Prerequisites:

- Ensure the SnapGear appliance is configured with a valid DNS server under one of its connections, since the appliance needs to resolve names in order for the URL filtering to operate. For more information, see “Connections” on page 35. You generally do not need to specify a DNS server for connections such as dial up serial, PPPoE ADSL, or for DHCP-assigned connections.
- Upload or copy and paste a certificate and private key. See “Uploading a Webwasher certificate and key” on page 321.

To enable and configure Webwasher URL filter service

- 1 From the **Firewall** menu, click **Access Control > Webwasher** tab > **Content Filtering** tab. The Webwasher URL Filter Service page appears.

Figure 236: Webwasher
URL Filter Service —
Content Filtering tab

Webwasher URL Filter Service

Main ACL Web Lists Policy Webwasher

Content Filtering Categories Reports Certificate Upload Certificate

Webwasher URL Filter Service

Both the certificate and the private key are missing or invalid.

Enable content filtering ☐

Allow accesses that cannot be rated ☐

Allow access to newly defined categories ☒

Identify users by account ☐

Enable Cache ☒

Submit

- 2 Select the **Enable content filtering** check box.
- 3 [Optional] To allow access to Web sites that the Webwasher filtering system has not yet rated, select the **Allow accesses that cannot be rated** check box. The default and recommended behavior is to block all unrated sites.
- 4 [Optional] Clearing the **Allow access to newly defined categories** check box restricts access to the categories you did not block when configuring content filtering. Selecting the check box allows access to any categories added after content filtering is configured.
- 5 [Optional] To send user names to the Webwasher reporting service, select the **Identify users by account** check box. In order for this field to have any effect, the **Require User Authentication** check box on the **Main** tab must be selected. For information, refer to “Enabling access control” on page 298. If you do not identify users by account, the reports are based upon IP addresses.

Note: If you want to bypass content filtering for a user, select the **Bypass content filtering** check box in the user's configuration (**System > Users > Local Users** tab). For more information, see “Adding a local user” on page 480. There are additional settings required to subject the user to other access controls. For more information, see article #2548 in the SnapGear knowledgebase: <http://sgkb.securecomputing.com>.

- 6 [Recommended] To cache the content rating results for improved performance, select the **Enable Cache** check box.
- 7 Click **Submit**.

Disabling Webwasher content filtering

- 1 From the **Firewall** menu, click **Access Control > Webwasher** tab > **Content Filtering** tab. The Webwasher URL Filter Service page appears.
- 2 Clear the **Enable content filtering** check box.
- 3 Click **Submit**.

Uploading a Webwasher certificate and key

Use this procedure to upload the Webwasher certificate and private key for your SnapGear appliance. Until you upload a valid certificate and key for the Webwasher filter service, the message “Both the certificate and the private key are missing or invalid” appears at the top of every Webwasher page. As an alternative to uploading, you can also copy and paste the certificate and private key information. See “Copying and pasting a Webwasher certificate and key” on page 322.

- 1 From the **Firewall** menu, click **Access Control > Webwasher** tab > **Certificate Upload** tab. The Certificate Upload page appears.

Figure 237: Webwasher URL Filter Service — Certificate Upload tab



The screenshot shows the 'Webwasher URL Filter Service' interface. At the top, there are tabs: 'Main', 'ACL', 'Web Lists', 'Policy', and 'Webwasher'. Under the 'Webwasher' tab, there are sub-tabs: 'Content Filtering', 'Categories', 'Reports', 'Certificate Upload', and 'Certificate'. The 'Certificate Upload' tab is selected. The main content area displays the message: 'Both the certificate and the private key are missing or invalid.' Below this message, there are two input fields: 'Certificate' and 'Private Key'. Each field has a 'Browse...' button next to it. At the bottom of the form is a 'Submit' button.

- 2 Click **Browse** to locate the certificate file, or enter the file name and path directly in the **Certificate** field.
- 3 Click **Browse** to locate the private key file, or enter the file name and path direct in the **Private Key** field.
- 4 Click **Submit**. The message that a valid certificate and private key are installed is displayed, along with the expiration date of the certificate, as shown in Figure 238.

Figure 238: Webwasher successful certificate upload



Copying and pasting a Webwasher certificate and key

Use this procedure to copy and paste a certificate and key into the text boxes provided if you received them in text format. Otherwise, use the Certificate Upload page. For instructions, see “Uploading a Webwasher certificate and key” on page 321.

- 1 From the **Firewall** menu, click **Access Control > Webwasher tab > Certificate** tab. The Certificate page appears.

Figure 239: Webwasher Certificate tab



- 2 Copy and paste the text into the **Certificate** and **Private Key** text boxes.



Important: Be sure to include both the *BEGIN CERTIFICATE* and *END CERTIFICATE* lines when copying and pasting text.

- 3 Click **Submit**.

Blocking categories for Webwasher filtering

Use this procedure to block categories for Webwasher filter service.

There is only one block or allow category policy per appliance. If necessary, you can override the Webwasher ratings in the **Web Lists** tab > **URL Allow** or **URL Block** pages. For more information, see “Web Lists tab” on page 307.

To block categories

- 1 From the **Firewall** menu, click **Access Control > Webwasher** tab > **Categories** tab. The Blocked Categories page appears.

Figure 240: Webwasher URL Filter Service — Blocked Categories tab



The screenshot shows the 'Webwasher URL Filter Service' interface. At the top, there are tabs: 'Main', 'ACL', 'Web Lists', 'Policy', and 'Webwasher'. Under the 'Webwasher' tab, there are sub-tabs: 'Content Filtering', 'Categories', 'Reports', 'Certificate Upload', and 'Certificate'. The 'Categories' sub-tab is selected, showing a section titled 'Blocked Categories'. Below this is a table with two columns: 'Category' and a checkbox column. The categories listed are: 'Pornography', 'Erotic/Sex', 'Swimwear/Lingerie/Nudity', 'Shopping', 'Auctions/Classified Ads', and 'Governmental Organizations'. All checkboxes are currently unchecked.

Category	
Pornography	<input type="checkbox"/>
Erotic/Sex	<input type="checkbox"/>
Swimwear/Lingerie/Nudity	<input type="checkbox"/>
Shopping	<input type="checkbox"/>
Auctions/Classified Ads	<input type="checkbox"/>
Governmental Organizations	<input type="checkbox"/>

- 2 Select the check boxes for the category or categories that you want to block. Clear the check box for any category you do not want to block. By default, all categories are unblocked initially.
- 3 Click **Submit**.

Viewing Webwasher reports

Use this procedure to view Webwasher URL filtering reports. You must have your username and password for your account. To use the reporting feature, you must have purchased the URL Filtering with Reporting license.

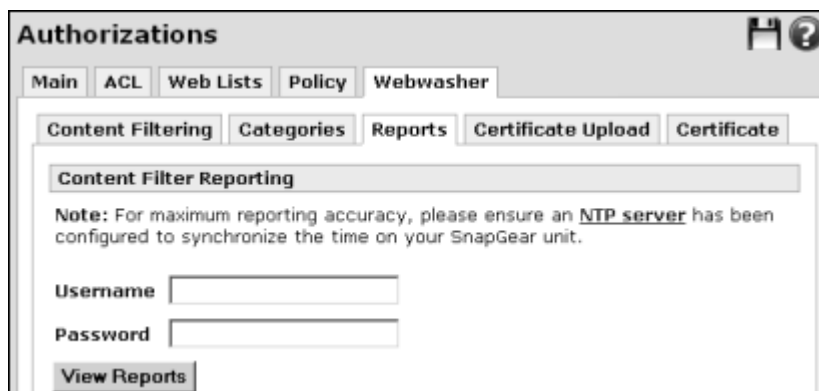
Prerequisites:

- 1 Enable and configure an NTP server for reporting accuracy. See “Enabling the NTP time server” on page 465.
- 2 Enter your certificate and private key for your Webwasher service into the SnapGear appliance with the method of your choice. See “Uploading a Webwasher certificate and key” on page 321 or “Copying and pasting a Webwasher certificate and key” on page 322.
- 3 Enable and configure Webwasher content filtering. See “Enabling Webwasher content filtering” on page 319.
- 4 Select the categories you want to block. See “Blocking categories for Webwasher filtering” on page 323.

To view Webwasher reports

- 1 From the **Firewall** menu, click **Access Control > Webwasher tab > Reports** tab. The Content Filter Reporting page appears.

Figure 241: Webwasher URL Filter Service — Reports tab



The screenshot shows the 'Authorizations' section of the SnapGear web interface. It has a top navigation bar with tabs: Main, ACL, Web Lists, Policy, and Webwasher. Under the 'Webwasher' tab, there are sub-tabs: Content Filtering, Categories, Reports, Certificate Upload, and Certificate. The 'Reports' sub-tab is selected, showing the 'Content Filter Reporting' section. This section contains a note about NTP server configuration, followed by input fields for 'Username' and 'Password', and a 'View Reports' button.

- 2 Enter your SnapGear account username into the **Username** field.
- 3 Enter your SnapGear account password into the **Password** field.
- 4 Click **View Reports**.

Testing a Webwasher URL rating

Use this procedure to test the URL rating of a given URL. You can provide feedback if you think the rating for the URL is inaccurate and needs to be reassessed.

- 1 Go to the following URL:

<https://www.securecomputing.com/goto/URLFilter>

The Webwasher URL Filter Tester page appears.

Figure 242: Webwasher
URL Filter Tester page

Webwasher URL Filter Tester **SECURE[®] COMPUTING**

Please use this URL-Feedback-System if you are running one of the following products:

- All Webwasher versions <= 6.0
- All Netcache versions with DynaBLocator

If you are using a SmartFilter product, please use the SmartFilter Where URL-Feedback-System at:
<http://www.securecomputing.com/sfwhere>

Please type in a URL to look up the URL Filter categorization.

You can also use the e-mail address ww_sites@securecomputing.com to send us URLs that are currently not in the URL Filter database or if you have any other questions to any URL categorizations.

Copyright © 2007 Secure Computing Corporation

2 Enter the URL and click **Check**. The results are displayed.

Figure 243: Webwasher
URL Filter Tester result

Webwasher URL Filter Tester

SECURE[®]
COMPUTING

Please use this URL-Feedback-System if you are running one of the following products:

- All Webwasher versions <= 6.0
- All Netcache versions with DynaLocator

If you are using a SmartFilter product, please use the SmartFilter Where URL-Feedback-System at:
<http://www.securecomputing.com/sfwhere>

Please type in a URL to look up the URL Filter categorization.

The URL <http://www.securecomputing.com/> is categorized as set forth:

before Webwasher 5.2 or on Netcache:

- Software / Hardware

since Webwasher 5.2 (not available on Netcache):

- Software / Hardware
- Business / Services

[URL Filter serial number: 1723]

If you disagree with this opinion, feel free to give us a notice by pressing the review button.
The URL will be submitted and reviewed as soon as possible.

Optional categorization suggestion:

Category 1

Category 2

Category 3

Optional comment:

3 You can suggest optional categories and add comments.

4 To submit your feedback, click **Review URL**.

Antivirus



Important: The antivirus feature applies to models SG565, SG580, and SG720 only. Due to the growth of antivirus signature databases, the SG565 and SG580 must be configured with external storage in order to enable antivirus. The SG565 can use local USB or network storage. For more information, see “Auxiliary storage for virus scanning” on page 330. If you are running firmware below version 3.1.5 and do not want to configure network storage for the SG720 but want to run antivirus in RAM only mode, Secure Computing strongly recommends increasing the size of the /var filesystem to 128 MB to prevent insufficient /var filesystem size. For instructions, refer to KB article #4864 at the following URL: <http://sgkb.securecomputing.com>.

The antivirus capabilities of the SnapGear appliance shield your LAN from viruses that propagate through email, the Web, and FTP. An antivirus subscription is not required and virus definitions are automatically kept up-to-date. The appliance is equipped with proxies for POP, SMTP, HTTP, and FTP that facilitate the transparent scanning of files passing through it.

If a virus is detected, the user on your LAN sending or receiving the infected file or email is informed by an error message or error email, and the infected file or email is not delivered to its destination. A message similar to the following is logged in the syslog:

```
E-Mail was blocked by pop3.proxy/2.0.0-beta5 using ClamAV
0.88/1516/Tue June 6 22:45:31
```

Note: If messages in your system log state your clamav is OUTDATED, it may be possible to update the virus scanning engine of the SnapGear appliance (ClamAV) by upgrading your SnapGear firmware. Typically, such messages are not cause for alarm and Antivirus still functions correctly. As with all firmware updates, Secure Computing determines an appropriate firmware release schedule based on the nature of the changes made. Serious vulnerabilities are given priority over feature enhancements.

If your SnapGear appliance is not connected to the Internet, the clam antivirus database files must be downloaded manually. For further information, see Appendix E, Downloading antivirus database files.

Once you enable antivirus scanning and allocate extra storage, configure antivirus for the areas you want to scan: SMTP or POP email, Web traffic, and FTP. The main topics in this section are as follows:

- “Enabling antivirus” on page 328
- “Auxiliary storage for virus scanning” on page 330
- “Virus scanning SMTP email” on page 336
- “Virus scanning POP email” on page 333
- “Virus scanning Web traffic” on page 337
- “Enabling FTP virus scanning” on page 338

Enabling antivirus

Use this procedure to enable and configure antivirus.



Important: For the SG565 and SG580 models, you must allocate extra memory for the scanning process. For more information, see “Auxiliary storage for virus scanning” on page 330.

- 1 From the **Firewall** menu, click **Antivirus**. The Antivirus Configuration page appears.

Figure 244: Anti-virus Configuration page

- 2 Select the **Enable** check box.
- 3 The **Database mirror** is the host from which the signature database is updated. Unless there is a specific host from which you want the SnapGear appliance to retrieve signature updates, leave this at the default setting of *database.clamav.net*.
- 4 Select the frequency to check for updates from the database mirror from the **Check for updates** list. The checks are quick and should not cause a noticeable decrease to performance unless an update is necessary. Available options are:
 - **Hourly**
 - **Daily**
 - **Weekly**

- 5 Specify the maximum size in kilobytes of files to scan for viruses in the **Maximum size** field. Files over this size are automatically rejected.
 - Default: 5120
 - Can be a value of 1 or greater
- 6 [Optional] To enable memory management for anti-virus, enter a value greater than zero (0) in the **Drop percentage** field. Specify the percentage of rules to ignore in the virus pattern database. Increasing this setting reduces the memory usage of the anti-virus subsystem at the risk of potentially missing a virus during scanning. Attempts to remove older rather than more recent signatures are made but this is not guaranteed. Use this field at your own risk, especially if you have an SG565 or SG580 that is experiencing memory problems due to the large and ever growing size of the clamav database.
 - Default: 0 (disabled)
 - Can be a value of 0 to 100%
- 7 [Optional] To treat encrypted content as a virus, select the **Treat encrypted content as virus** check box. Since the SnapGear appliance is not the intended recipient, it does not decrypt encrypted content passing through it, and cannot determine whether such content is infected.
- 8 Specify the **Maximum number of simultaneous virus checks** to perform. Permitting more scans increases the amount of memory and CPU resources required by the antivirus scanning.
 - Default: 20
 - Can be a value of 1 or greater
- 9 Click **Submit**.

Disabling antivirus

- 1 From the **Firewall** menu, click **Antivirus**. The Anti-Virus Configuration page appears.
- 2 Clear the **Enable** check box.
- 3 Click **Submit**.

Auxiliary storage for virus scanning

You can allocate extra local USB (SG565 only) or network storage for antivirus scanning. You can either designate a network share or local storage for antivirus purposes. Network and Local Shares for antivirus are mutually exclusive in that enabling one disables the other. Using a network or local share to provide storage for the virus database and temporary space for the scanning process greatly increases the effectiveness of the antivirus scanner for the SG720 and is required for its operation in the SG565 and SG580.



Important: For the SG565 and SG580 models, allocating extra memory for the scanning process is required.

Prerequisites:

- Create a network share if you have not already done so. See “Creating a Windows XP network share” on page 332.
- Create a dedicated user account (optional). See “Creating a Windows user account” on page 332.

Designating a network share for antivirus

- 1 From the **Firewall** menu, click **Antivirus > Storage** tab. The Network Storage page appears.

Figure 245: Antivirus
Network Storage

Network Storage

Antivirus Storage POP Email SMTP Email Web FTP

Network Storage Local Storage

Network Share

The antivirus scanner is capable of utilizing a network share to provide non-volatile storage for the virus database and temporary storage for the scanning process. Using this will greatly increase the effectiveness of the antivirus scanner.

(N.B. **Network Storage** and **Local Storage** cannot be used at the same time. Enabling one will automatically disable the other)

Use share ☐

Share

Username

Password

Confirm Password

Submit

- 2 Select the **Use share** check box.

- 3 Enter the path of the network share in the **Share** field. You can use the following formats:

`\\HOSTNAME\sharename` OR `\\a.b.c.d\sharename`

Note: Secure Computing recommends using a FQDN (Fully Qualified Domain Name) if specifying the hostname.

- 4 If you allowed full control to everyone on the network share drive, leave the Username and Password fields blank and click **Submit**. If the dedicated user account must authenticate to the network share, continue with step 5.
- 5 Enter the username of the user in the **Username** field. The user must be able to read to and write from the network share.
- 6 Enter the password for authentication with the network share in the **Password** field.
- 7 Enter the password again in the **Confirm Password** field. The password field entries must match.
- 8 Click **Submit**.

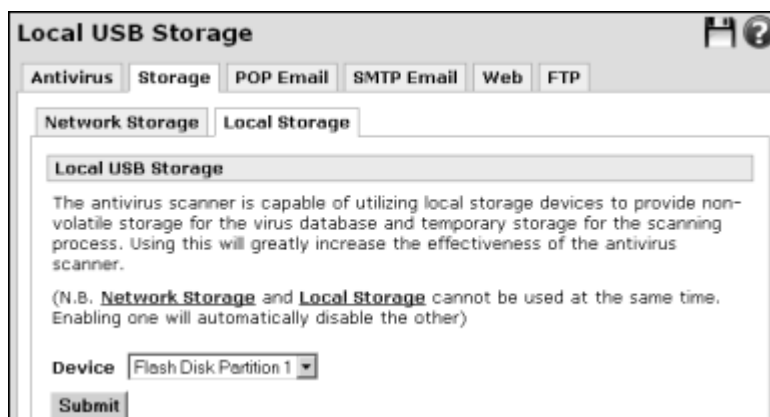
Designating local storage for antivirus

Note: Local storage is applicable to the SG565 model only. You must use either network or local storage for the SG565 model.

Use this procedure to select a local USB storage device for scanning memory. Attach a USB storage device to a SnapGear appliance USB port. For information about USB and partitioning USB storage devices, refer to Chapter 6, USB.

- 1 From the **Firewall** menu, click **Antivirus > Storage > Local Storage** tab. The Local USB Storage page appears.

Figure 246: Local USB Storage



The screenshot shows the 'Local USB Storage' configuration page. At the top, there are tabs for 'Antivirus', 'Storage', 'POP Email', 'SMTP Email', 'Web', and 'FTP'. Under the 'Storage' tab, there are sub-tabs for 'Network Storage' and 'Local Storage'. The 'Local Storage' sub-tab is selected. The main content area has a title 'Local USB Storage' and a description: 'The antivirus scanner is capable of utilizing local storage devices to provide non-volatile storage for the virus database and temporary storage for the scanning process. Using this will greatly increase the effectiveness of the antivirus scanner.' Below this, a note states: '(N.B. Network Storage and Local Storage cannot be used at the same time. Enabling one will automatically disable the other)'. There is a 'Device' dropdown menu currently set to 'Flash Disk Partition 1'. At the bottom, there is a 'Submit' button.

- 2 Select the USB device or partition from the **Device** list and click **Submit**.

Creating a Windows user account

It is recommended a special user account is created for use by the SnapGear appliance for reading and writing to the network share. If you have an existing account or want to make the network share readable and writable by everyone, you can disregard this procedure. This procedure is for the Windows XP operating system. Refer to Microsoft documentation for current information and more detail.

- 1 Click **Start > Control Panel > User Accounts > Create a new account**. Type a name for the new account; for example *sguser*, and click **Next**.
- 2 Typically it is sufficient to grant this account **Limited** privileges.
- 3 Click **Create Account**.
- 4 Select the account you have just created under **Pick an account to change**.
- 5 Select **Create a password**. Enter and confirm a password for this account, as well as a password hint if desired.

Creating a Windows XP network share

A network share is a shared folder or drive on a local Windows PC, or a PC running another operating system capable of SMB sharing such as Mac OS X, or a Linux PC running the SAMBA service. For details on creating a network share on an OS other than Windows, refer to the documentation for your operating system.

- 1 Launch Windows Explorer (**Start > (All) Programs > Accessories > Windows Explorer**) and open up a folder or drive to dedicate as a network share for use by the SnapGear appliance.
- 2 Begin by disabling simple file sharing for this folder. From the **Tools** menu, select **Folder Options**. Click the **View** tab and under the **Advanced settings** section clear **Use simple file sharing (Recommended)**. Click **OK**.
- 3 Next, share the folder. Right-click the folder and select **Sharing and Security**. Select **Share this folder** and note the **Share name**; you can change this to something easier to remember if desired.
- 4 Finally, to set the security permissions of the newly created network share, click **Permissions**.
- 5 [Recommended] If you want to secure the network share with a user name and password, click **Add** and type the user name the account to be used by the SnapGear appliance and click **Check Names** then **OK**.
- 6 Select this account, or **Everyone** if you are not securing the network share with a user name and password, and check **Allow** next to **Full Control**. Click **OK** and **OK** again to finish.

Virus scanning POP email

The SnapGear appliance can scan email being sent by PCs on your LAN before delivering it to the destination mail server.

Note: *Scanning of IMAP and Web-based email is not supported.*

The POP Email page allows you to configure a transparent POP3 proxy that virus checks incoming email before passing it to a real POP3 server for delivery to its addressee. In the majority of cases, minimal changes will be required at each client POP application. When scanning finds a virus within a message attachment, the POP3 proxy strips the attachment and body from the email and, in a rewritten message, passes the original mail headers through to the original recipient, notifying them of the virus detection.

This service is configured differently depending on whether you want to scan all incoming email, or scan only email being retrieved by specific PCs on your LAN.

Figure 247: Pop-Based Email

The screenshot shows the 'POP Based Email' configuration page. At the top, there are tabs for 'Antivirus', 'Storage', 'POP Email' (which is selected), 'SMTP Email', 'Web', and 'FTP'. The page contains several configuration options:

- Virus check POP based email:** A checkbox that is checked.
- Default POP server:** An empty text input field.
- Allow connections to other POP servers:** A checkbox that is checked.
- Transparent:** A checkbox that is checked.
- Request timeout (seconds):** A text input field containing the value '600'.
- Identification:** A text input field containing the value 'SnapGear Anti-Virus'.
- Reduce syslog output:** A checkbox that is checked.

At the bottom left of the form is a 'Submit' button. In the top right corner of the window, there is a help icon (a question mark inside a circle).

Virus scanning all POP email

For each email client that is not retrieving e-mail from the default POP server (this may be all email clients), the email client's POP3 user name setting must be in the form of `user@mail.isp.com`, rather than simply "user" — `user` is the POP3 login, and `mail.isp.com` is the POP3 mail server.

- 1 From the **Firewall** menu, click **Antivirus > POP Email** tab. The POP Based Email page appears.
- 2 Select the **Virus check POP based email** check box.
- 3 Depending on your mail server environment, follow the appropriate steps below:
 - If all of your internal email clients (such as Microsoft Outlook) are retrieving email from a single mail server only:
 - Enter it as the **Default POP server**.
 - Clear the **Allow connections to other POP servers** check box.
 - If most, but not all, of your internal email clients are retrieving email from a single mail server:
 - Enter this as the **Default POP server**.
 - Select the **Allow connections to other POP servers** check box.
 - If there is no single mail server from which most of your internal email clients are retrieving email:
 - Leave the **Default POP server** field blank.
 - Select the **Allow connections to other POP servers** check box. The check box must be selected if the Default POP server field is blank.
- 4 [Optional] To enable a transparent mode of operation, select the **Transparent** check box. When enabled, all POP3 network traffic crossing the appliance is transparently proxied. The proxy server initiates connections on behalf of the original user and virus checks incoming email messages.
- 5 [Optional] Adjust the number of seconds elapsed before a timeout in the **Request timeout** field. Typically, it is not necessary to adjust the default value for POP3 protocol.
 - Default: 600
 - Can be a value of 1 or greater
- 6 [Optional] To customize the text in the blocked message notification, enter a string in the **Identification** field. The name indicates the sender of the notification.
 - Default: SnapGear Anti-Virus
- 7 [Optional] Once you determine POP scanning is functioning properly, reduce syslog output by selecting the **Reduce syslog output** check box.
- 8 Click **Submit**.

Scanning POP email for specific clients only

For each of the email clients for which to scan incoming mail, the email client's POP3 user name setting must be in the form of `user@mail.isp.com`, rather than simply "user" – `user` is the POP3 login, and `mail.isp.com` is the POP3 mail server. Additionally, the email client's incoming/POP3 email server setting must be sent to the SnapGear appliance's LAN IP address (for example, 192.168.0.1).

- 1 From the **Firewall** menu, click **Antivirus > POP Email** tab.
- 2 Select the **Virus check POP based email** check box.
- 3 Leave **Default POP server** blank.
- 4 Select the **Allow connections to other POP servers** check box.
- 5 Clear the **Transparent** check box.
- 6 Typically it is not necessary to adjust the default value for POP3 protocol **Request timeout** field.
- 7 Once POP scanning is functioning properly, select the **Reduce syslog output** check box to reduce syslog output.
- 8 Click **Submit**.

Virus scanning SMTP email

If you have an SMTP mail server on your LAN, the appliance antivirus can scan emails sent to it by external mail servers.

- 1 From the **Firewall** menu, click **Antivirus > SMTP Email** tab. The SMTP-Based Email page appears.

Figure 248: SMTP-Based Email

SMTP Based Email

Antivirus Storage POP Email **SMTP Email** Web FTP

Virus check SMTP based email ☐

Send keep alive bytes to requesting server ☐

Inform requesting server of rejected mail ☒

Destination SMTP server

Source NAT connections ☒

Network timeout (seconds)

Maximum simultaneous SMTP sessions

Submit

- 2 [Optional] Select the **Virus check SMTP based email** check box.
- 3 [Optional] To send keep alive traffic to the source SMTP server, select the **Send keep alive bytes to requesting server** check box. This option is only useful on slow network connections where the source server is timing out before the appliance has finished its virus checking.
- 4 [Recommended, enabled by default] To reject incoming mail with a virus detected, select the **Inform requesting server of rejected mail** check box. The appliance informs the requesting SMTP server when mail has been dropped.

When the check box is cleared, the appliance accepts and then subsequently drops incoming mail detected to contain a virus. The requesting mail server is unaware the mail was not delivered. The appliance drops the mail without notification to the sender or requesting server.
- 5 Enter your SMTP mail server address of your LAN in the **Destination SMTP server** field.
- 6 [Enabled by default] To enable source address translation, select the **Source NAT connections** check box. This enabled option prevents your mail server from being turned into an open relay if it is configured to trust and forward messages appearing to originate from the LAN address of the appliance. If enabled, the apparent source address for connections to the internal SMTP server is one of the WAN addresses for the appliance. If disabled, the apparent source address is from the LAN side of the appliance. An *open relay* configuration allows anyone on the Internet to send email through your appliance.

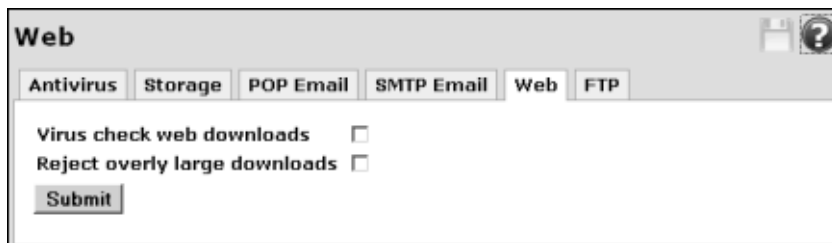
- 7 If you are experiencing timeout problems, adjust the value in the **Network timeout** field. Typically, the default is adequate.
 - Default: 180 (seconds)
 - Can be a value of 1 or greater
- 8 To set the maximum number of simultaneous SMTP connections, enter a value in the **Maximum simultaneous SMTP sessions** field. Increasing this value increases the resources consumed by virus scanning.
 - Default: 10
 - Can be a value of 1 or greater
- 9 Click **Submit**.

Virus scanning Web traffic

The SnapGear appliance can scan incoming Web traffic for viruses.

- 1 From the **Firewall** menu, click **Antivirus > Web** tab. The Antivirus Web page appears.

Figure 249: Antivirus
Web tab

The screenshot shows a web interface titled "Web" with a help icon in the top right corner. Below the title is a row of tabs: "Antivirus", "Storage", "POP Email", "SMTP Email", "Web", and "FTP". The "Web" tab is currently selected. Under the "Web" tab, there are two checkboxes: "Virus check web downloads" and "Reject overly large downloads", both of which are currently unchecked. Below these checkboxes is a "Submit" button.

- 2 Select the **Virus check Web downloads** check box. You must have access control enabled for this to function. For more information on access control, see "Enabling access control" on page 298.
- 3 To treat oversized downloads as potential viruses and reject them, select the **Reject overly large downloads** check box. The definition of an overly large download is specified by the **Maximum size** field on the main **Antivirus** tab. See "Enabling antivirus" on page 328.
- 4 Click **Submit**.

Enabling FTP virus scanning

Use this procedure to enable and configure virus scanning. FTP transfers going through the appliance are proxied and scanned for viruses.

- 1 Click **Firewall > Antivirus > FTP** tab. The FTP page appears.

Figure 250: FTP virus scanning

The screenshot shows the 'FTP' configuration page. At the top, there are tabs for 'Antivirus', 'Storage', 'POP Email', 'SMTP Email', 'Web', and 'FTP'. The 'FTP' tab is active. Below the tabs, the configuration options are as follows:

Configuration Option	Value
Virus check ftp downloads	<input checked="" type="checkbox"/>
Proxy port	2121
No activity timeout (seconds)	300
Maximum simultaneous connections	0
Maximum connections for one host	400
Keep alive interval (0 = disabled)	30

A 'Submit' button is located at the bottom left of the configuration area.

- 2 To enable FTP downloads virus checking, select the **Virus check FTP downloads** check box.
- 3 Typically there is no need to change the default proxy port on which the transparent proxy listens for connections. If necessary, enter a different port for the FTP proxy in the **Proxy port** field.
 - Default: 2121
 - Range: 1-65535
- 4 Enter a value to determine disconnecting idle FTP connections in the **No activity timeout** field. If an FTP connection is idle for the number of seconds specified, the connection is automatically disconnected. Increase this only if you are experiencing timeouts during FTP sessions.
 - Default: 300
 - Can be a value of 1 or greater
- 5 Specify the maximum number of simultaneous connections to allow in the **Maximum simultaneous connections** field. This is the total number of FTP connections allowed from your LAN. Once this number is reached, subsequent FTP connections are rejected until previous FTP connections are disconnected. More resources are consumed by virus scanning when a higher number of simultaneous FTP connections are established.
 - Default: 10
 - Can be a value of 0 or greater

- 6 Specify the maximum connections allowed for one host in the **Maximum connections for one host** field. This is the number of FTP connections allowed from a single PC. Once this number is reached, subsequent FTP connections are rejected until previous FTP connections are disconnected. This value should not exceed the Maximum simultaneous connections value.
 - Default: 4
 - Can be a value of 1 or greater
- 7 To keep an FTP download from timing out, enter an interval value to send a status message in the Keep alive interval field. If an FTP client cannot process the status messages, disable the feature by entering zero (0).
 - 0: disables the Keep alive interval feature
 - Default: 30
 - Can be a value of 0 or greater
- 8 Click **Submit**.

Antispam (TrustedSource)

TrustedSource is a reputation service that filters incoming mail connections. The service provides precise information about the reputation of an e-mail sender based on their IP address. The TrustedSource reputation service is a tool for reducing the amount of spam that reaches the inboxes of your organization. However, unlike spam filters that evaluate message content, TrustedSource focuses on a sender's reputation score. A reputation score is similar to a credit score in that it indicates a sender's trustworthiness. With TrustedSource, the lower the score, the more trustworthy the sender.

Note: *This add-on module is currently available for evaluation. Contact your Secure Computing channel partner or sales representative for additional information. TrustedSource filtering will not function on the appliance until it is licensed.*

About TrustedSource

To determine reputation scores, TrustedSource uses servers around the world to gather and analyze messages. TrustedSource assigns a score to an IP address based on the type of mail (legitimate or spam) that a particular host generates. The score ranges from negative (-)140 to positive (+)140. The SnapGear administrator can configure a score that represents a tolerable threshold for your network. If a sender's score is higher than your threshold, messages from that sender are rejected by the SnapGear appliance. The TrustedSource servers are in constant communication, so as one server identifies a spam flood in progress, it can alert all TrustedSource servers moments after the attack starts, and update the offending sender's reputation score.

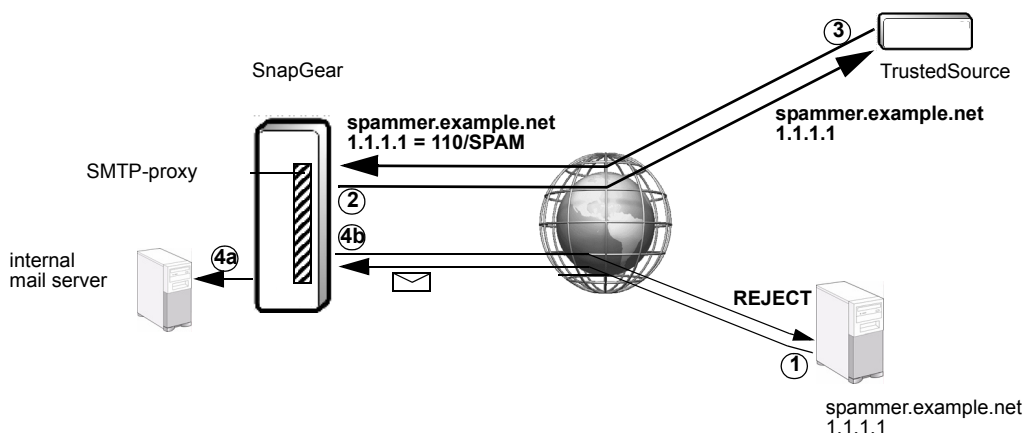
For more information on TrustedSource, visit www.trustedsource.org.

The steps in the TrustedSource process are enumerated below:

- 1 A sending mail server contacts a SnapGear appliance running mail via SMTP-proxy.
- 2 The appliance sends a modified DNS query that includes the sending mail server's IP address to a TrustedSource server to get its reputation score.
- 3 The TrustedSource server sends the score to the appliance.
- 4 The appliance compares the score to the threshold value and takes one of the following actions:
 - a If the score is lower than the threshold, e-mail messages from the server are accepted and forwarded to the internal mail servers.
 - b If the score is higher than the threshold, the appliance rejects the message, logs the violation, and closes the connection.

This process is illustrated in Figure 251:

Figure 251:
TrustedSource query
example



Licensing is handled by the TrustedSource server. Once enabled, TrustedSource automatically starts filtering all inbound mail; you do not need to alter the existing rules or create new rules.



Important: You should not create a port forward or destination NAT rule to allow incoming SMTP if you are using TrustedSource. If you are not using TrustedSource, NAT or port forward rules may be required to allow incoming SMTP.

TrustedSource Reputation Scores

Trustworthy senders receive low scores and untrustworthy senders receive high scores ranging from -140 to +140. The delineating values and corresponding descriptions are described in Table 20:

Table 20: TrustedSource reputation classes

Value	Description
< 0 (negative values)	Inoffensive.
0 through 14	Neutral
15 through 29	Unverified
30 through 49	Suspicious
50 or greater	Malicious

Enabling TrustedSource

Use the following procedure to enable and configure TrustedSource for the SnapGear appliance. The mail server must be configured as an SMTP-proxy.



Security Alert: Since anti-virus for SMTP e-mail and TrustedSource share SMTP resources, only one SMTP server can be protected by these features.

Prerequisites:

Ensure that your appliance meets the following criteria:

- DNS is configured with access to the Internet. Refer to “DNS” on page 153.
- The SnapGear appliance is located on the perimeter of your network and is not behind another firewall.
- Be sure you have entered the serial number of your SnapGear appliance in the “Entering device settings” on page 151. The serial number of the appliance is used as the serial number for the TrustedSource licensing and is required to enable TrustedSource in a SnapGear appliance.
- You have registered your appliance and activated the feature. For more information, see “Registering your SnapGear appliance” on page 15, “Activating a feature” on page 16.

To enable TrustedSource filtering

- 1 Select **Firewall > Antispam > TrustedSource** tab. The TrustedSource page appears.

Figure 252: Antispam
TrustedSource page

Antispam

TrustedSource TrustedSource Tests

TrustedSource Antispam Configuration

Enable TrustedSource ☐

Reputation Threshold

Destination SMTP server

Source NAT connections ☒

Network timeout (seconds)

Maximum simultaneous SMTP sessions

Debug Level

Submit

- 2 Select the **Enable TrustedSource** check box.
- 3 Set the reputation value in the **Reputation Threshold** field. Messages from senders with reputation scores above that value are rejected. For more information, see “TrustedSource Reputation Scores” on page 342.
 - Default: 80
 - Range: -140 through +140
- 4 Enter your SMTP mail server address of your LAN in the **Destination SMTP server** field.
- 5 [Optional] To enable source address translation, select the **Source NAT connections** check box. This enabled by default option prevents your mail server from being turned into an open relay if it is configured to trust and forward messages appearing to originate from the LAN address of the appliance. If enabled, the apparent source address for connections to the internal SMTP server is one of the WAN addresses for the appliance. If disabled, the apparent source address is from the LAN side of the appliance. An *open relay* configuration allows anyone on the Internet to send email through your appliance.
- 6 If you are experiencing timeout problems, adjust the value in the **Network timeout** field. Typically, the default is adequate.
 - Default: 180 (seconds)
 - Can be a value of 1 or greater

- 7 To set the maximum number of simultaneous SMTP connections, enter a value in the **Maximum simultaneous SMTP sessions** field. Increasing this value increases the resources consumed by TrustedSource filtering.
 - Default: 10
 - Can be a value of 1 or greater
- 8 In the **Debug Level** field, enter a value for the debugging level in the System Log
 - Valid range: 1 (least verbose) through 4 (most verbose). Levels 3 and 4 display the TrustedSource scores in the Syslog.
 - Default: 1
- 9 Click **Submit**.

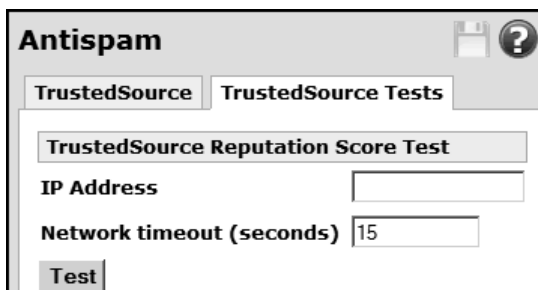
The appliance now uses the TrustedSource reputation service to filter inbound e-mail. You can test the configuration in the TrustedSource Tests page.

Testing TrustedSource

Use this procedure to test your TrustedSource configuration. The TrustedSource Tests page allows you to test the configuration of your TrustedSource query engine. You can also use this page to query the reputation of a given server, which allows you to more finely-tune your reputation threshold. If this test is failing to return a reputation, it could mean that your SnapGear appliance has not been registered for TrustedSource correctly or that your DNS settings are not correct. There may be a delay for your TrustedSource license to become activated. Please allow four (4) hours for your license to become activated.

- 1 Select **Firewall > Antispam > TrustedSource Tests** tab. The TrustedSource Reputation Score Test page appears.

Figure 253: Antispam — TrustedSource Tests page



- 2 Enter the **IP address** for which the test will attempt to get a TrustedSource rating.
 - Format: a.b.c.d

- 3 [Optional] Adjust the number of seconds in the **Network Timeout** field. This value defines the timeout for network activity. Typically, the default is adequate and should only be changed if there are timeout issues. A value of zero (0) disables the timeout specified in this page and defaults to any internal timeout values present in the network infrastructure.
 - Default: 15.
 - Allowed values: Must be a value of zero (0) or greater.
- 4 Click **Test**. A successful test returns a rating. An unsuccessful test returns a reputation retrieval failed message, which could be due to either the license not being activated or an invalid IP address being entered.

Disabling TrustedSource

- 1 Select **Firewall > Antispam > TrustedSource** tab. The TrustedSource page appears.
- 2 Clear the **Enable** check box.
- 3 Click **Submit**.

CHAPTER 4

VPN

In this chapter...

About VPN.....	348
PPTP VPN Client	349
PPTP VPN Server	352
L2TP VPN Server.....	363
L2TP VPN Client	373
About IPSec VPN	376
IPSec Advanced Setup wizard	387
Setting up the branch office.....	410
Certificate management	420
IPSec failover	435
IPSec VPN offloading	444
Troubleshooting IPSec	447
Port tunnels	452

About VPN

VPN (Virtual Private Networking) enables two or more locations to communicate securely and effectively, usually across a public network such as the Internet. VPN has the following key traits:

- **Privacy** — No one else can see what you are communicating.
- **Authentication** — You know who you are communicating with.
- **Integrity** — No one else can tamper with your messages or data.

Using VPN, you can access the office network securely across the Internet using PPTP (Point-to-Point Tunneling Protocol), IPSec, or L2TP. If you take your portable computer on a business trip, you can dial a local number to connect to your Internet access service provider (ISP) and then create a second connection (called a *tunnel*) into your office network across the Internet and have the same access to your corporate network as if you were connected directly from your office. Similarly, telecommuters can also set up a VPN tunnel over their cable modem or DSL links to their local ISP.

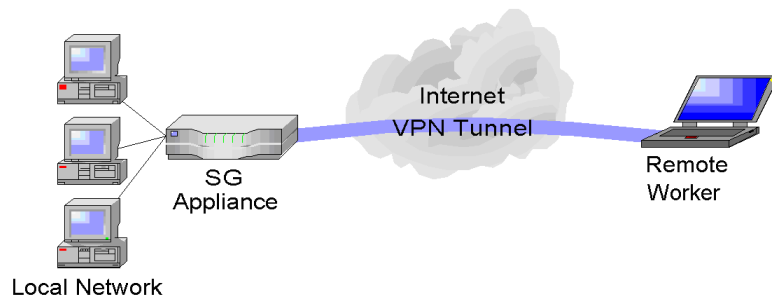
VPN technology can be deployed as a low cost way of securely linking two or more networks, such as a headquarters LAN to the branch offices. IPSec is generally the most suitable choice in this scenario.

With the SnapGear appliance, you can establish a VPN tunnel over the Internet using either PPTP, IPSec, or L2TP. IPSec provides enterprise-grade security, and is generally used for connecting two or more networks, such as a branch office to a head office. The strength of PPTP is its ease of configuration and integration into existing Microsoft infrastructure. It is generally used for connecting single remote Windows clients.

L2TP combines elements of IPSec and PPTP. It is generally used as a relatively easy way to configure a PPTP-style connection from a remote Windows XP client with IPSec security.

This chapter details how to configure the L2TP and PPTP servers and clients, how to configure a remote client to connect, how to establish an IPSec tunnel, and provides an overview of L2TP VPN tunneling. The SnapGear appliance includes a PPTP and an L2TP VPN server. These allow remote Windows clients to securely connect to the local network as shown in Figure 254:

Figure 254: VPN example



PPTP or L2TP are also commonly used to secure connections from a guest network. For more information, see “Guest network” on page 97.

About PPTP

PPTP is typically used for communications over a physical or virtual serial link. The PPP endpoints define a virtual IP address to themselves. Routes to networks can then be defined with these IP addresses as the gateway, which results in traffic being sent across the tunnel. PPTP establishes a tunnel between the physical PPP endpoints and securely transports sessions data across the tunnel.

PPTP consists of two protocols:

- TCP port 1723 is used for establishing the tunnel and managing the GRE tunnel
- GRE (Generic Routing Encapsulation) IP protocol 47 is used for encrypting and encapsulating PPP session data over GRE

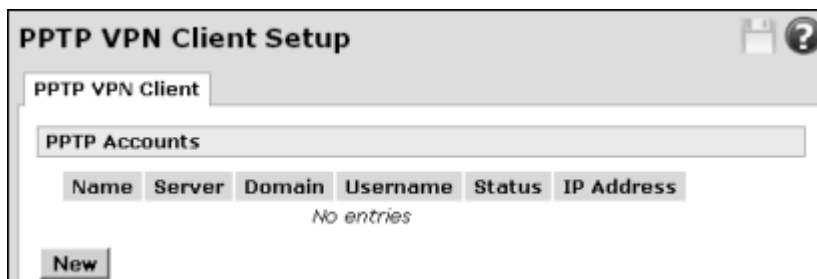
The SnapGear appliance can operate as a PPTP client or a PPTP server. The configuration of the appliance defines which networks are accessible via the tunnel. The appliance initiates the PPTP tunnel with a specified PPTP server. The SnapGear appliance configured as a PPTP client acts as the local gateway for users behind the firewall. When the appliance operates as a PPTP server, a remote client initiates the PPTP tunnel. The appliance authenticates the client. A remote client can be a Windows device for single user access, or it can be a gateway such as another SnapGear appliance configured as a PPTP client, thereby allowing multiple user access.

PPTP VPN Client

Use this procedure to configure a PPTP VPN client. The PPTP client enables the SnapGear appliance to establish a VPN to a remote network running a PPTP server, usually a Microsoft Windows server.

- 1 From the **VPN** menu, click **PPTP VPN Client**. The PPTP VPN Client Setup page appears.

Figure 255: PPTP VPN Client Setup page



- 2 Click **New**. The Edit VPN Connection page appears.

Figure 256: Edit (PPTP)
VPN Connection page

Edit VPN Connection

PPTP VPN Client

Edit VPN Connection

Enable ☒

Name

Server

Domain

Username

Password

Confirm Password

Subnet Mask for Remote network

PPTP MTU

Use Peer DNS ☐

NAT ☐

Make VPN the Default Route (single VPN only) ☐

Finish **Cancel**

- 3 Ensure the **Enable** check box is selected. It is selected by default.
- 4 Enter a description of the VPN connection in the **Name** field. This can describe the purpose for the connection.
- 5 Enter the address of the remote PPTP Server to connect to in the **Server** field. Allowed formats are as follows:
 - Can be a fully-qualified domain name 'host.domain.com'.
 - Each label (host or domain) can consist of alphabetic, numeric or hyphen '-' characters.
 - Each label cannot begin or end with the hyphen '-' character.
 - Can be an IP address in the form a.b.c.d
- 6 [Optional] Enter a Windows domain name in the **Domain** field to use for authentication with the server.
- 7 Enter a username in the **Username** field to use when logging in to the remote VPN. You may need to obtain the username and password information from the system administrator of the remote PPTP server. The username cannot start with @.
- 8 Enter the password in the **Password** field to use when logging in to the remote VPN. The password can be one or more characters of any type.
- 9 Enter the password again in the **Confirm Password** field.

- 10** [Optional] To indicate which packets should go the remote network, enter a netmask number between 0 and 32 in the **Subnet Mask for Remote network** field. The netmask can also be written in the form 255.255.255.0.

***Tip:** When you configure the Subnet Mask for Remote network, the PPTP Client connection automatically adds a route to a remote network based on the IP address it receives from the server. This is useful if you have services other than the remote PPTP server you want to access using the PPTP tunnel. It is recommended to set this value of the network mask to the remote network.*

You can also configure additional static routes accessible over the PPTP client VPN. Do not specify a gateway, and select the PPTP client connection in the Interface field. For more information on static routes, see “Creating a static route” on page 139.

- 11** The Maximum Transmission appliance (MTU) of the PPTP interface can be configured by entering the desired value in the **PPTP MTU** field.
- Can be an integer equal to or greater than 1
 - Default: 1400
- 12** [Optional] To use any DNS servers returned by the remote PPTP VPN server, select the **Use Peer DNS** check box.
- 13** [Optional] To masquerade your local network behind the IP address on the remote network that the remote PPTP server allocates the SnapGear appliance, select the **NAT** check box.
- 14** [Optional] If you have a single VPN and want traffic from your local network to be routed through the tunnel instead of straight out onto the Internet, select the **Make VPN the default route (single VPN only)** check box.
- 15** Click **Finish**. A PPTP status icon appears in the system tray informing you that you are connected. You can now check your e-mail, use the office printer, access shared files and computers on the network as if you were physically on the LAN.

Depending on how your remote network is set up, some additional configuration may be required to enable browsing the network (such as **Network Neighborhood** or **My Network Places**). For further details, refer to article **#2730** in the SnapGear knowledgebase:
<http://sgkb.securecomputing.com>.

To disconnect, right-click the PPTP Status system tray icon and select **Disconnect**.

PPTP VPN Server

To set up a PPTP connection from a remote Windows client to your SnapGear appliance and local network:

- 1** Enable and configure the PPTP VPN server. See “Enabling and configuring the PPTP VPN Server” on page 353.
- 2** Set up VPN user accounts on the SnapGear appliance and enable the appropriate authentication security. See “Adding a PPTP user account” on page 355.
- 3** Configure the VPN clients at the remote sites. The client does not require special software—the SnapGear PPTP Server supports the standard PPTP client software included with Windows 95/98, Windows ME, Windows XP, Windows NT, and Windows 2000. The SnapGear PPTP server is also compatible with UNIX PPTP client software. See “Setting up a Windows XP PPTP client” on page 356.
- 4** Connect to the remote VPN client. See “Setting up the remote PPTP client” on page 356.

Enabling and configuring the PPTP VPN Server

Use this procedure to enable and configure the SnapGear appliance as a PPTP VPN Server.

- 1 From the **VPN** menu, click **PPTP VPN Server**. The PPTP VPN Server Setup page appears.

Figure 257: PPTP Server Setup page—basic view

PPTP VPN Server Setup

PPTP VPN Server

PPTP Server Setup

Enable PPTP Server ☒

IP addresses to give to remote hosts

IP Address to Assign VPN Server

Authentication Scheme

Required Encryption Level

Authentication Database

- 2 To access the Advanced fields, click **Advanced**. Additional fields become available for your use.

Figure 258: PPTP Server Setup page—Advanced view

PPTP VPN Server Setup

PPTP VPN Server

PPTP Server Setup

Enable PPTP Server ☒

IP addresses to give to remote hosts

IP Address to Assign VPN Server

Authentication Scheme

Required Encryption Level

Authentication Database

PPTP MTU

Idle Time (minutes)

DNS Server

WINS Server

- 3 Select the **Enable PPTP Server** check box.
- 4 Enter the free IP Address or range in the **IP Addresses to give to remote hosts** field. This must be a free IP address, or a range of free IP addresses, from the network (typically the LAN) that remote users are assigned while connected to the SnapGear appliance.

***Tip:** If required, you can specify a static IP address for a given PPTP user when you create the local user for PPTP access. The user must also be allocated a dynamic address. For further information, see “Adding a PPTP user account” on page 355 and “Adding a local user” on page 480.*

- 5 If you have configured several network connections, select the one that you want to connect remote users to from the **IP Address to Assign VPN Server** list. This is typically a LAN interface or alias.
- 6 Select the weakest **Authentication Scheme** to accept. Access is denied to remote users attempting to connect using an authentication scheme weaker than the selected scheme. The schemes are described below, from strongest to weakest.
 - **Encrypted Authentication (MS-CHAP v2):** The strongest type of authentication to use; this is the recommended option.
 - **Encrypted Authentication (MS-CHAP):** This is not a recommended encryption type and should only be used for older dial-in clients that do not support MS-CHAP v2.
 - **Weakly Encrypted Authentication (CHAP):** This is the weakest type of encrypted password authentication to use. It is not recommended that clients connect using this as it provides very little password protection. Also note that clients connecting using CHAP are unable to encrypt traffic.
 - **Unencrypted Authentication (PAP):** This is plain text password authentication. When using this type of authentication, the client password is transmitted unencrypted.
- 7 Select the **Required Encryption Level**. Access is denied to remote users attempting to connect not using this encryption level. **Strong Encryption (MPPE 128 Bit)** is recommended.
- 8 Select the user authentication location from the **Authentication Database** list. This allows you to indicate where the list of valid clients can be found. You can select from the following options:
 - **Local:** Use the local database defined on the **Local Users** tab of the **Users** page. You must enable the **Dial-in Access** option for the individual users that are allowed dial-in access.
 - **RADIUS:** Use an external RADIUS server as defined on the **RADIUS** tab of the **Users** page.
 - **TACACS+:** Use an external TACACS+ server as defined on the **TACACS+** tab of the **Users** page.

For further details on users, RADIUS, and TACAS+, refer to “Users menu” on page 476.

- 9 [Optional] To configure Advanced options, click **Advanced**. The following fields are available:
 - a Enter the desired value of the Maximum Transmission appliance (MTU) for the PPTP interfaces into the **PPTP MTU** field.
 - Default: 1400
 - b Enter the number of minutes without activity before disconnecting the PPTP client in the **Idle Time (minutes)** field.
 - c In the **DNS Server** field, enter the IP address of the DNS server that assigns IP addresses to connecting PPTP clients.
 - d In the **WINS Server** field, enter the IP address of the WINS server that assigns IP addresses to connecting PPTP clients.
- 10 Click **Submit**.

Adding a PPTP user account

Use this procedure to add a new PPTP VPN user. Keep a note of the User name and Password, as these are required in configuring the remote PPTP client.

- 1 Click **System > Users > Local Users** tab. The Local Users page is displayed.
- 2 Click **New**. The Edit User Information page appears.
- 3 Complete the fields. For further details on adding a user, refer to “Adding a local user” on page 480. Keep note of the username and password for when you need to connect to the VPN connection.
- 4 [Required for VPN PPTP access] Be sure to select the **PPTP Access** check box.
- 5 If applicable, enter a static IP address in the **PPTP Address** field.
- 6 Click **Finish**.

Setting up the remote PPTP client

To connect remote VPN clients to the local network, you need to know the user name and password for the PPTP account you added, as well as the Internet IP address of the SnapGear appliance. Your Internet IP address is displayed on the Network Setup page (see Figure 23 on page 35). If your ISP has not allocated you a static IP address, consider using a dynamic DNS service. Otherwise, you must modify the PPTP client configuration each time your Internet IP address changes. For details on configuring dynamic DNS, refer to the “Dynamic DNS tab” on page 155. Ensure the remote VPN client PC has Internet connectivity.

To create a VPN connection across the Internet, you must set up two networking connections. One connection is for the ISP, and the other connection is for the VPN tunnel to your office network. The PPTP server of the appliance interoperates with the standard Windows PPTP clients in all current versions of Windows.

Setting up a Windows XP PPTP client

Use this procedure to set up a PPTP client in the Windows XP Professional operating system. The steps may vary slightly depending on your network access, such as if you are using a Smart Card, or if you are using standard Windows XP rather than XP Professional. More detailed instructions are available in the Windows product documentation, and from the Microsoft Web site.

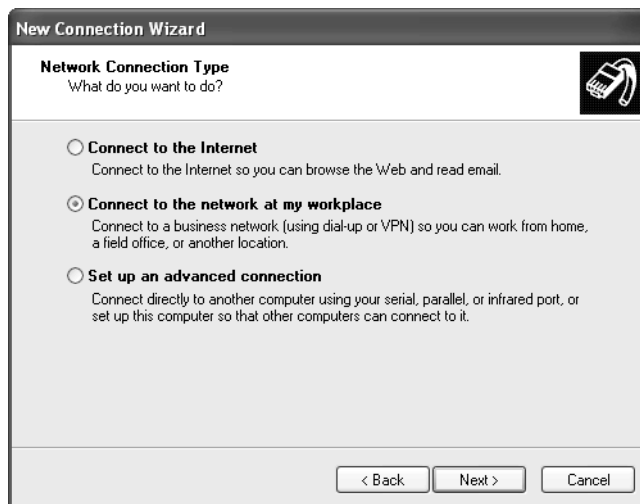
- 1 Login with administrator privileges.
- 2 From the **Start** menu, click **Settings > Network Connections**.
- 3 Click **Create New Connection** from the **Network Tasks** menu. The New Connection Wizard begins.

Figure 259: New Connection Wizard Welcome page



- 4 Select **Connect to the network at my workplace** and click **Next**.

Figure 260: New Connection Wizard Network Connection Type page



- 5 Select **Virtual Private Network connection** and click **Next**.

Figure 261: Connection Wizard Network Connection page



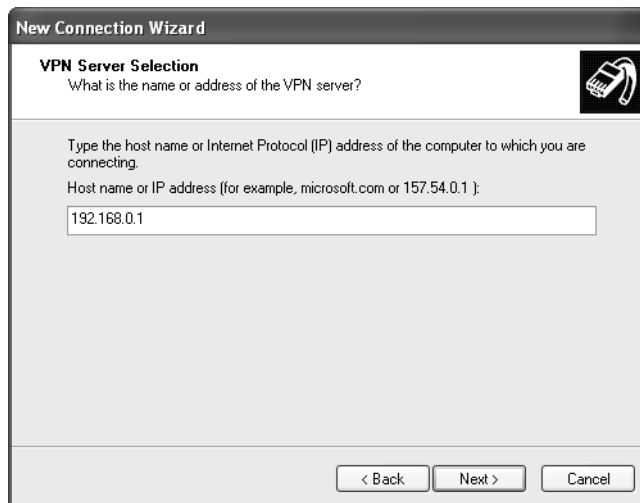
- 6** Enter a **Connection Name** for the VPN connection, such as your company name or simply *Office*. Click **Next**.

Figure 262: Connection Wizard Connection Name page



- 7** [Conditional] If you have set up your computer to connect to your ISP using dial up, select **Automatically dial this initial connection** and your dial-up account from the list. If not, or if you wish to manually establish your ISP connection before the VPN connection, select **Do not dial the initial connection**. Click **Next**.

Figure 263: Connection Wizard VPN Server Selection page



New Connection Wizard

VPN Server Selection
What is the name or address of the VPN server?

Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.
Host name or IP address (for example, microsoft.com or 157.54.0.1) :

192.168.0.1

< Back Next > Cancel

- 8 Enter the SG PPTP appliance's Internet IP address or fully qualified domain name and click **Next**.

Figure 264: Connection Wizard Availability page



New Connection Wizard

Connection Availability
You can make the new connection available to any user or only to yourself.

A connection that is created for your use only is saved in your user account and is not available unless you are logged on.
Create this connection for:

☐ Anyone's use
☒ My use only

< Back Next > Cancel

- 9 Select whether you want to make this connect available to all users or only yourself and click **Next**.

Figure 265: Connection Wizard Completion page



- 10 To add a shortcut to your desktop, select the check box and click **Finish**. Your VPN client is now set up and ready to connect. The Connect dialog box is displayed.

Figure 266: VPN connection



- 11 Verify that you are connected to the Internet, or have set up your VPN connection to automatically establish an initial Internet connection.
- 12 Enter a user name and password added in the "Adding a PPTP user account" on page 355.
- 13 Click **Connect**.

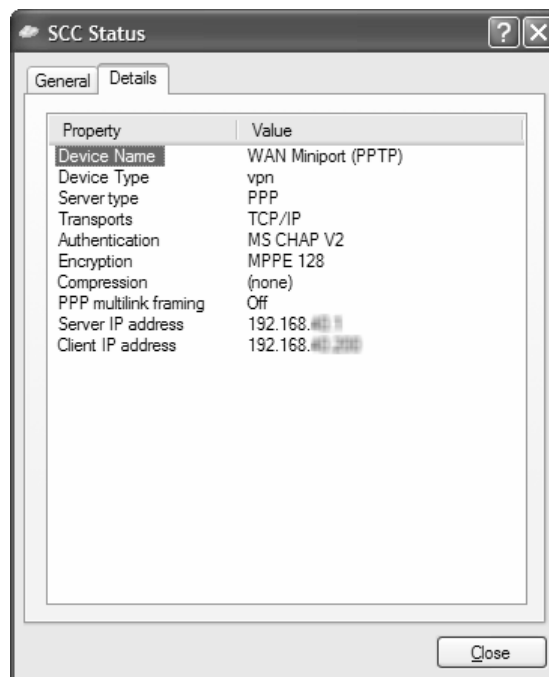
Figure 267: VPN connection



Right-click on the VPN connection to connect, view its status when connected, and make other changes as desired.

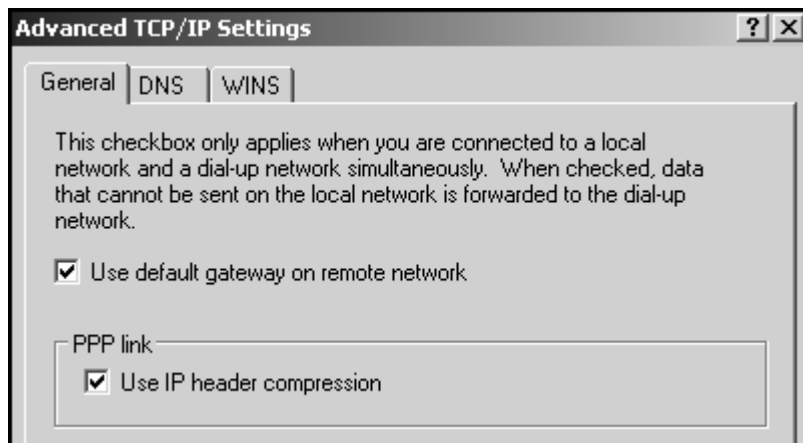
Figure 268 displays the status of a connection named “SCC.”

Figure 268: Viewing CPN connection status details



Tip: By default, Microsoft Windows sets the PPTP client connection to be the default gateway. As a result, all Internet traffic requested by the PPTP client will also travel via the PPTP server, not just internal corporate traffic, which may adversely affect the PPTP server Internet link performance. To disable this setting, edit the properties of the PPTP client connection: Select the **Networking tab > TCP/IP Properties > Advanced >** and ensure you clear the **Use default gateway on remote network** option. Beware this may affect routing and may cause complications if you are trying to access internal corporate servers that are not on the same internal subnet as the SnapGear PPTP server.

Figure 269: Use default gateway option



L2TP VPN Server

To set up an L2TP/IPSec connection from a remote Windows XP client to your SnapGear appliance and local network, perform the following procedures:

- 1 Enable and configure the L2TP VPN server. See “Configuring the L2TP VPN server” on page 363.
- 2 Configure the L2TP IPSec tunnel settings. See “L2TP IPSec Configuration page” on page 366, “Authenticating tunnels with an x.509 certificate” on page 368, and “Authenticating tunnels with a preshared secret” on page 369.
- 3 Set up VPN user accounts on the SnapGear appliance and enable the appropriate authentication security. See “Adding an L2TP user account” on page 370.
- 4 Configure the VPN clients at the remote sites. The client does not require special software, since the SnapGear L2TP Server supports the standard L2TP and IPSec client software included with Windows XP. See “Configuring the remote L2TP client” on page 371.

Note: *The L2TP Server does not currently support tunnels with Microsoft clients when there is a device in between the client and the SnapGear appliance performing NAT.*

- 5 Connect to the remote VPN client. See “Connecting to the remote VPN client” on page 372.

Configuring the L2TP VPN server

Use this procedure to enable and configure the L2TP server for VPN.

- 1 From the **VPN** menu, click **L2TP VPN Server**. The L2TP VPN Server Setup page appears.

Figure 270: L2TP VPN
Server Setup page

L2TP VPN Server Setup

L2TP VPN Server | **L2TP IPsec Configuration**

L2TP Server Setup

Enable L2TP Server ☐

IP addresses to give to remote hosts

IP Address to Assign VPN Server

Authentication Scheme

Required Encryption Level

Authentication Database

L2TP MTU

Submit

- 2 Select the **Enable L2TP Server** check box.
- 3 Enter the **IP addresses to give to remote hosts**. This must be a free IP address, or a range of free IP addresses, from the network (typically the LAN) that the remote users are assigned while connected to the SnapGear appliance. Can be an IP address range of the following forms:
 - a.b.c.d
 - a.b.c.d-e
 - a.b.c.d-e.f.g.h
 - a.b.c.d/e
 - a.b.c.d/e.f.g.h
 - a.b.c.d+e

Tip: If required, you can specify a static IP address for a given L2TP user when you create the local user for L2TP access. For further information, see “Adding an L2TP user account” on page 370.

- 4 If you have configured several network connections, select the one that you want to connect remote users to from the **IP Address to Assign VPN Server** list. This is typically a LAN interface or alias.

- 5 Select the weakest **Authentication Scheme** to accept. Access is denied to remote users attempting to connect using an authentication scheme weaker than your selection. They are described below, from strongest to weakest:
 - **Encrypted Authentication (MS-CHAP v2) — [Recommended]** The strongest type of authentication to use.
 - **Encrypted Authentication (MS-CHAP)** — This is not a recommended encryption type and should only be used for older dial-in clients that do not support MS-CHAP v2.
 - **Weakly Encrypted Authentication (CHAP)** — This is the weakest type of encrypted password authentication to use. It is not recommended that clients connect using this as it provides very little password protection. Also note that clients connecting using CHAP are unable to encrypt traffic.
 - **Unencrypted Authentication (PAP)** — This is plain text password authentication. When using this type of authentication, the client passwords are transmitted unencrypted over the Internet.
- 6 Select the **Required Encryption Level**. Access is denied to remote users attempting to connect not using this encryption level. Using **Strong Encryption (MPPE 128 Bit)** is recommended.
- 7 Select the **Authentication Database**. This allows you to indicate where the list of valid clients can be found. You can select from the following options:
 - **Local** — Use the local database defined on the **Local Users** tab of the **Users** page. You must enable the L2TP Access option for the individual users that are allowed L2TP access.
 - **RADIUS** — Use an external RADIUS server as defined on the **RADIUS** tab of the **Users** page.
 - **TACACS+** — Use an external TACACS+ server as defined on the **TACACS+** tab of the **Users** page.

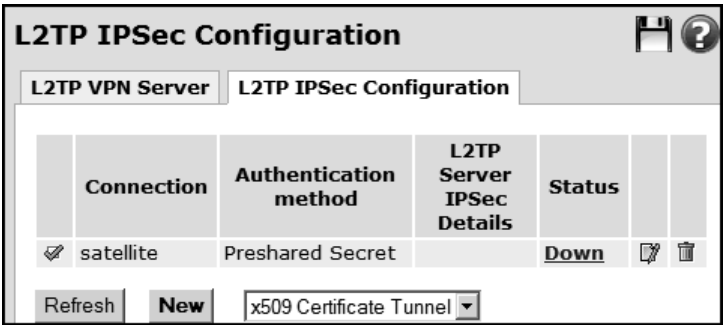
For details on adding user accounts for PPTP access, and configuring the SnapGear appliance to enable authentication against a RADIUS or TACACS+ server, see “Users menu” on page 476.
- 8 Enter the desired value of the Maximum Transmission (MTU) for the L2TP interfaces into the **L2TP MTU** field.
 - Default: 1400
- 9 Click **Submit**.

L2TP IPSec Configuration page

Use this page to create an IPSec tunnel for use with L2TP. Authentication is performed using x.509 certificates or a preshared secret. You can add a single shared secret tunnel for *all* remote clients authenticating using shared secrets, an x.509 certificate tunnel for *each* remote client authenticating using certificates, or both.

- Select **Shared Secret Tunnel** to use a common secret (passphrase) that is shared between the SnapGear appliance and the remote client. This authentication method is relatively simple to configure, and relatively secure.
- Select **x.509 Certificate Tunnel** to use x.509 certificates to authenticate the remote client against a Certificate Authority's (CA) certificate. The CA certificate must have signed the local certificates that are used for tunnel authentication. Certificates need to be uploaded to the SnapGear appliance before a tunnel can be configured to use them. For instructions, see "Adding a certificate for use with IPSec VPN" on page 431. This authentication method is more difficult to configure, but very secure.

Figure 271: L2TP IPSec Configuration page



L2TP Server IPsec Details — If the authentication method is x.509 certificates, this column shows the distinguished name of the remotely connecting device.

Status — Click the linked text to view more details about the status, as shown in Figure 272 on page 367. Click **Refresh** to update the current status.

Viewing the status of an L2TP IPsec tunnel

- 1 From the **VPN** menu, click **L2TP VPN Server > L2TP IPsec Configuration** tab.
- 2 Click the linked status. The configuration displays data similar to that shown in Figure 272:

Figure 272: L2TP IPsec status (down)

L2TP IPsec Configuration

L2TP VPN Server
L2TP IPsec Configuration

Interfaces Loaded

```
000 interface ipsec0/eth1 10.10.
000 interface ipsec0/eth1 10.10.
```

Phase 2 Ciphers Loaded

```
000 algorithm ESP encrypt: id=2,
000 algorithm ESP encrypt: id=3,
000 algorithm ESP encrypt: id=12
```

Phase 2 Hashes Loaded

```
000 algorithm ESP auth attr: id=
000 algorithm ESP auth attr: id=
```

Phase 1 Ciphers Loaded

```
000 algorithm IKE encrypt: id=7,
000 algorithm IKE encrypt: id=5,
000 algorithm IKE encrypt: id=1,
```

Phase 1 Hashes Loaded

```
000 algorithm IKE hash: id=2, na
000 algorithm IKE hash: id=1, na
```

Diffie Hellman Groups Loaded

```
000 algorithm IKE dh group: id=1
000 algorithm IKE dh group: id=2
000 algorithm IKE dh group: id=5
000 algorithm IKE dh group: id=4
000 algorithm IKE dh group: id=4
000 algorithm IKE dh group: id=4
```

Update
Cancel

- 3 Click **Update** to update the current status.
- 4 When you are done viewing the information, click **Cancel** to cancel out of the status and return to the L2TP IPsec configuration page.

For further information about the IPsec status information, see “IPsec status details overview” on page 384.

Authenticating tunnels with an x.509 certificate

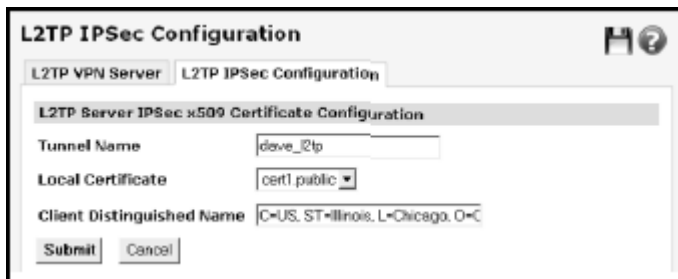
Use this procedure to create an IPSec connection over an L2TP VPN tunnel.

Prerequisite: Upload certificates to the SnapGear appliance. See “Certificate management” on page 420.

Multiple x.509 certificate tunnels can be added. A separate x.509 certificate tunnel is required for each remote client to authenticate.

- 1 From the **VPN** menu, click **L2TP VPN Server > L2TP IPSec Configuration** tab.
- 2 Select **x509 Certificate Tunnel** from the configuration list and click **New**.
 - If there are no local certificates available to use, you are prompted to either go to the Certificate Lists page to upload it, or to click **Cancel** and create a shared secret tunnel instead.
 - If there are x.509 certificates available, the L2TP Server IPSec x509 Certificate Configuration page appears.

Figure 273: L2TP IPSec Certificate Configuration



The screenshot shows a web-based configuration interface titled "L2TP IPSec Configuration". It has two tabs: "L2TP VPN Server" and "L2TP IPSec Configuration", with the latter being active. Below the tabs is a sub-header "L2TP Server IPSec x509 Certificate Configuration". The form contains three fields: "Tunnel Name" with the value "dave_@tp", "Local Certificate" with a dropdown menu showing "cert1 public", and "Client Distinguished Name" with the value "C=US, ST=Illinois, L=Chicago, O=C". At the bottom are "Submit" and "Cancel" buttons.

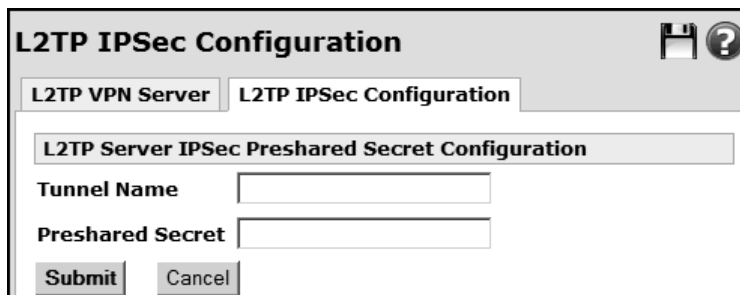
- 3 Enter a name to identify the connection in the **Tunnel Name** field. The name must be unique and not the same as any other L2TP/IPSec or regular IPSec tunnel names.
- 4 From the **Local Certificate** list, select the certificate uploaded to the SnapGear appliance.
- 5 Enter the **Client Distinguished Name**. It must match exactly the distinguished name of the remote party's local certificate to successfully authenticate the tunnel. Distinguished name fields are listed within the field.
- 6 Click **Submit**. The connection is added to the list, and the Distinguished name displays in the **Details** column.

Authenticating tunnels with a preshared secret

Use this procedure to create an IPsec tunnel for an L2TP connection. Only one shared secret tunnel can be created. The one shared secret is used by all remote clients to authenticate. When using preshared secrets with an L2TP tunnel, a single Main Mode connection with a remote dynamic endpoint is configured. Only a single Main Mode dynamic connection is supported so that multiple L2TP clients can use this tunnel to connect. Creating a preshared secret L2TP tunnel means that IPsec cannot be configured with any Main Mode tunnels to a dynamic remote endpoint that uses preshared secrets. You must either use Aggressive mode, x509 certificates, or RSA digital signatures.

- 1 From the **VPN** menu, click **L2TP VPN Server > L2TP IPsec Configuration** tab.
- 2 Select **Preshared Secret Tunnel** from the configuration list and click **New**. The L2TP IPsec Preshared Secret Configuration page appears.

Figure 274: L2TP Server
IPsec Preshared Secret
Configuration



The screenshot shows a web interface titled "L2TP IPsec Configuration". At the top, there are two tabs: "L2TP VPN Server" and "L2TP IPsec Configuration", with the latter being selected. Below the tabs is a sub-header "L2TP Server IPsec Preshared Secret Configuration". The form contains two input fields: "Tunnel Name" and "Preshared Secret". At the bottom of the form are two buttons: "Submit" and "Cancel".

- 3 Enter a **Tunnel Name** to identify this connection. The name is used as an identifier by the IPsec subsystem and must be unique across all L2TP and normal IPsec tunnels.
- 4 Enter the **Preshared Secret**. Ensure it is something hard to guess. Keep note of the shared secret, as it is used in configuring the remote client. This field contains the preshared secret that allows each of the endpoints to verify the identity of the other endpoint. It must match at both endpoints.
- 5 Click **Submit**. The server is added to the list.

Deleting an L2TP IPsec tunnel configuration

- 1 From the **VPN** menu, click **L2TP VPN Server > L2TP IPsec Configuration** tab.
- 2 Click the delete icon for the tunnel you want to delete.

Adding an L2TP user account

Use this procedure to add a new L2TP user to the configuration of the SnapGear appliance. Keep a note of the User name and Password, as these are required in configuring the remote L2TP client.

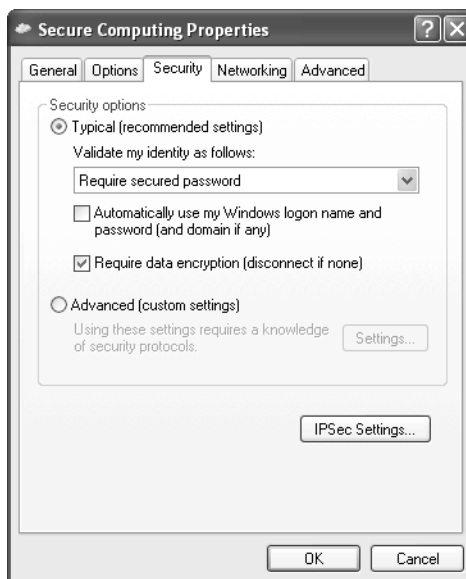
- 1** Click **System > Users > Local Users** tab. The Local Users page is displayed.
- 2** Click **New**. The Edit User Information page appears.
- 3** Complete the fields. For further details, refer to “Adding a local user” on page 480.
- 4** [Required for VPN L2TP access] Be sure to select the **L2TP Access** check box.
- 5** If applicable, enter a static IP address in the **L2TP Address** field.
- 6** Click **Finish**.

Configuring the remote L2TP client

The following instructions are for Windows XP.

- 1 Login with administrator privileges.
- 2 From the **Start** menu, select **Settings** and then **Network Connections**.
- 3 Click **Create New Connection** from the **Network Tasks** menu to the left.
- 4 Select **Connect to the network at my workplace** and click **Next**. Select **Virtual Private Network connection** and click **Next**.
- 5 Choose a **Connection Name** for the VPN connection, such as your company name or simply *Office*. Click **Next**.
- 6 If you have set up your computer to connect to your ISP using dial up, select **Automatically dial this initial connection** and your dial up account from the list. If not, or if you want to manually establish your ISP connection before the VPN connection, select **Do not dial the initial connection**. Click **Next**.
- 7 Enter the SG L2TP appliance's Internet IP address or fully qualified domain name and click **Next**. Select whether you want make this connection available to all users and whether you want to add a shortcut to your desktop and click **Finish**.
 - To authenticate using a **Shared Secret Tunnel**, click **Properties** on the **Connect Connection Name** dialog box.

Figure 275: Connection Security Properties



- Click **Security** > **IPSec Settings**.

- Select the **Use pre-shared key for authentication** check box and in the **Key** field, enter the **Shared Secret** you indicated when configuring the shared secret tunnel on the SnapGear appliance.

Figure 276: L2TP Server
IPSec Preshared Secret
Configuration



- To authenticate using an **x.509 Certificate Tunnel**, you must first install the local certificate. The distinguished name of this local certificate must match the name entered in **Client Distinguished Name** when configuring the x.509 certificate tunnel on the SnapGear appliance. See “Certificate management” on page 420 for details on creating, packaging, and adding certificates for use by Windows IPSec. Once a certificate is added, Windows IPSec automatically uses it to attempt to authenticate the connection. If more than one certificate is installed, it tries each of them in turn. Authentication fails if the Windows client’s certificate and the SnapGear appliance’s certificate are not signed by the same CA (Certificate Authority).

Your VPN client is now set up and ready to connect.

Connecting to the remote VPN client

Verify that you are connected to the Internet, or have set up your VPN connection to automatically establish an initial Internet connection.

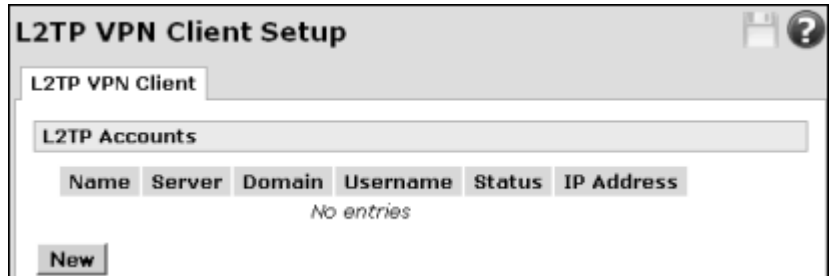
- 1 In **Network Connections**, right-click the connection for the SnapGear appliance VPN and click **Connect**. The Connect dialog box appears.
- 2 Enter a user name and password added in the procedure “Adding an L2TP user account” on page 370.
- 3 Click **Connect**.

L2TP VPN Client

The L2TP client enables the SnapGear appliance to establish a VPN to a remote network running an L2TP server, which is usually a Microsoft Windows server.

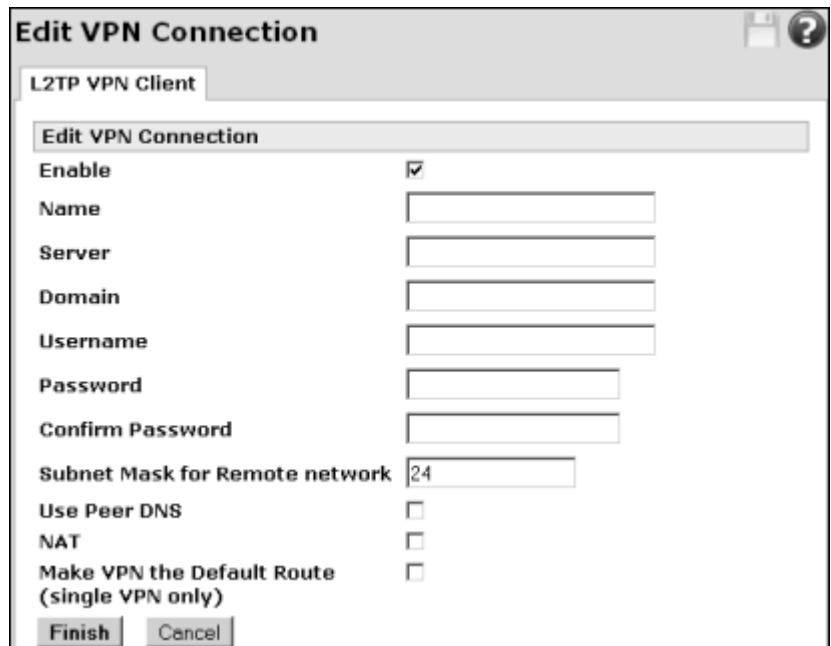
- 1 From the **VPN** main menu, click **L2TP VPN Client**. The L2TP VPN Client Setup page appears.

Figure 277: L2TP VPN Client Setup page



- 2 Click **New**. The Edit VPN Connection page appears.

Figure 278: Edit L2TP VPN Connection page



- 3 Ensure the **Enable** check box is selected. It is selected by default.
- 4 Enter a descriptive name for the VPN connection, such as the purpose of the connection, in the **Name** field.

- 5 Enter the address of the remote L2TP Server to connect to in the **Server** field. Allowed formats are as follows:
 - Can be a fully-qualified domain name 'host.domain.com'.
 - Each label (host or domain) can consist of alphabetic, numeric or hyphen '-' characters.
 - Each label cannot begin or end with the hyphen '-' character.
 - Can be an IP address in the form a.b.c.d
- 6 Enter a username in the **Username** field to use when logging in to the remote VPN. You may need to obtain the username and password information from the system administrator of the remote PPTP server. The username cannot start with @.
- 7 Enter the password in the **Password** field to use when logging in to the remote VPN. The password can be one or more characters of any type.
- 8 Enter the password again in the **Confirm Password** field.
- 9 [Optional] To indicate which packets should go the remote network, enter a netmask number between 0 and 32 in the **Subnet Mask for Remote network** field. The netmask can also be written in the form 255.255.255.0.

***Tip:** When you configure the Subnet Mask for Remote network, the L2TP Client connection automatically adds a route to a remote network based on the IP address it receives from the server. This is useful if you have services other than the remote L2TP server you want to access using the L2TP tunnel. It is recommended to set this value of the network mask to the remote network.*

You can also configure additional static routes accessible over the L2TP client VPN. Do not specify a gateway, and select the L2TP client connection in the interface field. For more information on static routes, see "Creating a static route" on page 139.

- 10 [Optional] To use any DNS servers returned by the remote L2TP VPN server, select the **Use Peer DNS** check box.
- 11 [Optional] To masquerade your local network behind the IP address on the remote network that the remote L2TP server allocates the SnapGear appliance, select the **NAT** check box.
- 12 [Optional] If you have a single VPN and want traffic from your local network to be routed through the tunnel instead of straight out onto the Internet, select the **Make VPN the default route (single VPN only)** check box.
- 13 Click **Finish**. A L2TP status icon appears in the system tray informing you that you are connected.

You can now check your e-mail, use the office printer, access shared files and computers on the network as if you were physically on the LAN.

Depending on how your remote network is set up, some additional configuration may be required to enable browsing the network (such as **Network Neighborhood** or **My Network Places**).

For further details, refer to article **#2730** in the SnapGear knowledgebase:

<http://sgkb.securecomputing.com>

To disconnect, right-click the L2TP Status system tray icon and click **Disconnect**.

About IPSec VPN

IPSec is the most widely used form of VPN. Unlike PPTP and L2TP, IPSec is governed by RFCs and is not specific to any particular vendor,. IPSec is typically implemented as a client-gateway or gateway-gateway application.

An IPSec tunnel connects two endpoints. These endpoints may be of different types; however, some configurations are preferable to others with regards to ease of configuration and security (i.e., main vs. aggressive mode) and robustness (i.e., relying on an external DNS server). The following is a list of configurations, from most to least preferable, remote to local location:

- 1 Static IP address to static IP address
- 2 Dynamic IP address to static IP address (as detailed in “IPSec example” on page 410)
- 3 DNS hostname address to static IP address
- 4 DNS hostname address to DNS hostname address
- 5 DNS hostname address to dynamic IP address

Authentication

The SnapGear appliance supports the following types of authentication:

- **Preshared Secret** is a common secret (passphrase) that is shared between the SnapGear appliance and the remote party. This authentication method is widely supported, relatively simple to configure, and relatively secure, although it is somewhat less secure when used with aggressive mode keying.
- **RSA Digital Signatures** uses a public/private RSA key pair for authentication. The SnapGear appliance can generate these key pairs. The public keys need to be exchanged between the SnapGear appliance and the remote party in order to configure the tunnel. This authentication method is not widely supported, but is relatively secure and allows dynamic endpoints to be used with main mode keying. Use this authentication method if you want more security than preshared secrets. This method is also preferable over x.509 certificates *unless* you require the ability to expire the certificate automatically after a specified period of time, or desire a third party to sign certificates rather than self-sign. In those cases, x.509 certificate authentication is mandatory.
- **x.509 Certificates** are used to authenticate the remote party against a Certificate Authority's (CA) certificate. The CA must have signed the local certificates that are used for tunnel authentication. Certificates need to be uploaded to the SnapGear appliance before a tunnel can be configured to use them (see “Certificate management” on page 420). This authentication method is widely supported and very secure; however, differing terminology between vendors can make it difficult to set up a tunnel between a SnapGear appliance and an appliance from another vendor. This authentication method allows dynamic endpoints to be used with main mode keying.

IPSec VPN Setup page

Use this page to configure the appliance to allow IPSec tunnels to connect to or initiate from the appliance. This page also shows a list of all of the IPSec connections configured on the appliance.

Figure 279: IPSec VPN Setup General Settings

The screenshot shows the 'IPSec VPN Setup' page with two tabs: 'IPSec' (selected) and 'Certificate Lists'. Under 'IPSec General Settings', there is a checkbox for 'Enable IPSec' which is checked, and a text input for 'IPSec MTU'. A 'Submit' button is below these. The 'Tunnel List' section contains a table with three columns: 'Connection', 'Remote Party', and 'Status'. There are three rows of tunnels, each with a checkmark in the first column. The first row has 'n' as the connection name and '0.0.0.0' as the remote party. The second row has 'tunnel_secret' and 'sg@remote.com'. The third row has 'test_cert' and a longer distinguished name. All three tunnels are listed with a 'Down' status. At the bottom of the table are buttons for 'Refresh', 'Quick Setup', and 'Advanced'.

Connection	Remote Party	Status
✓ n	0.0.0.0	Down
✓ tunnel_secret	sg@remote.com	Down
✓ test_cert	C=US, ST=MN, O=SecureComputing, CN=remoteoffice.securecomputing.com, emailAddress=vpn@securecomputing.com	Down

Once populated with tunnels, the **Tunnel List** pane displays the following information:

- **Connection** — This is the user-defined name for the IPSec tunnel connection.
- **Remote Party** — This is the identity of the IPSec tunnel's remote endpoint. It is defined either by its Endpoint ID, IP Address, or Distinguished Name.
- **Status** — Tunnels that use Automatic Keying (IKE) will have one of several states in this field. The states include the following:
 - **Down** indicates that the tunnel is not being negotiated. This may be due to the following reasons:
 - IPSec is disabled
 - The tunnel is disabled
 - The tunnel could not be loaded due to misconfiguration
 - **Negotiating Phase 1** indicates that IPSec is negotiating Phase 1 to establish the tunnel. Aggressive or Main mode packets (depending on tunnel configuration) are transmitted during this stage of the negotiation process.
 - **Negotiating Phase 2** indicates that IPSec is negotiating Phase 2 to establish the tunnel. Quick mode packets are transmitted during this stage of the negotiation process.

- **Running** indicates that the tunnel has been established.
- **Running, Renegotiating Phase 1** indicates that the tunnel has been established and the tunnel is attempting to renegotiate its Phase 1 keys.
- **Running, Renegotiating Phase 2** indicates that the tunnel has been established and the tunnel is attempting to renegotiate its Phase 2 keys.

Further negotiation details can be seen by clicking on the **status** link. Click **Refresh** to refresh the statistics.

Note: *Tunnels that use manual keying are in either a Down or Running state.*

To create a basic IPSec tunnel connection, click **Quick Setup**. The Quick Setup is appropriate and recommended for an IPSec tunnel between two SnapGear appliances that both have static IP addresses. To create an IPSec tunnel connection using advanced settings, click **Advanced**.

Procedures you can perform on this page include:

- “Enabling IPSec VPN” on page 378
- “Creating an IPSec tunnel with Quick Setup” on page 379
- “Refreshing status of IPSec VPN tunnels” on page 382
- “Disabling an IPSec VPN tunnel” on page 386
- “Disabling IPSec VPN” on page 386
- “Deleting an IPSec VPN tunnel” on page 386
- “IPSec Advanced Setup wizard” on page 387

Enabling IPSec VPN

Use this procedure to enable IPSec VPN.

- 1 From the **VPN** menu, click **IPSec**. The IPSec VPN Setup page appears.
- 2 Select the **Enable IPSec** check box.

[Optional] Enter an MTU (Maximum Transmission Unit) value in the **IPSec MTU** field. For most applications, this need not be configured and can be left blank. If set, the MTU value should be between 1400 and 1500. For details on determining the optimal MTU setting, refer to knowledgebase article **#2748** in the SnapGear Portal <http://sgkb.securecomputing.com>.

- 3 Click **Submit**.

Creating an IPSec tunnel with Quick Setup

This procedure uses the Quick Setup to connect two sites together that have static IP addresses. For more control over the configuration options, see “Setting up the branch office” on page 410.

- 1 From the **VPN** menu, click **IPSec**. The IPSec VPN Setup page appears.
- 2 Click **Quick Setup**. The Tunnel Settings page appears.

Figure 280: IPSec VPN Setup — Tunnel Settings page — Preshared Secret

- 3 Fill in the **Tunnel name** field with your name for the tunnel. The name must not contain spaces or start with a number. For example, enter *Headquarters*.
- 4 Leave the **Enable this tunnel** check box selected.
- 5 Enter **The remote party's IP address**, which is the IP address of the remote party's IPSec endpoint. For a remote party that has a dynamic IP address, click **Predefined** and **dynamic IP address** appears in the list.
- 6 Enter the **Local Network** that will have access to the remote network. Either select from a list of predefined values, which are based on the current network configuration, or click **Custom** to define custom networks.
- 7 Enter the **Remote Network** that the specified local network should have access to. Click **Predefined** to choose Remote Endpoint or other existing definitions.
- 8 From the **Authentication** list, select one of the following:

- **Preshared Secret** — Default. This is a common secret (passphrase) that is shared between the device and the remote party. Tunnels configured with this method of authentication using the Quick Setup will by default use the Aggressive Mode of keying.

Note: *Preshared Secret is the only authentication currently supported by VPN offloading.*

- **X.509 Certificates** — are used to authenticate the remote party against a Certificate Authority's (CA) certificate. The CA certificate must have signed the local certificates that are used for tunnel authentication. Local and CA Certificates need to be uploaded to the device before a tunnel can be configured to use them. Tunnels configured with this method of authentication using the Quick Setup will by default use the Main Mode of keying. If you select this option, skip to step 12
- 9 [Conditional; only if **Preshared Secret** was selected for **Authentication**] Enter the **Local Endpoint ID** using the form of an email to authenticate the device to the remote party. For example: sg@local.com.
 - 10 [Conditional; only if **Preshared Secret** was selected for **Authentication**] Enter the **Remote Endpoint ID** using the form of an email to authenticate the device to the remote party. For example: sg@remote.com.
 - 11 [Conditional; only if **Preshared Secret** was selected for **Authentication**] Enter the **Preshared Secret** to use during negotiations. This secret should be kept confidential.
 - 12 [Conditional; only if **x.509 Certificates** was selected for **Authentication**] Enter the **Remote Distinguished Name**, which is the list of attribute/value pairs contained in the certificate of the remote peer.

Table 21 provides a list of supported attributes.

Table 21: Supported attributes

Attribute	Description
C	County
ST	State or province
L	Locality or town
O	Organization
OU	Organizational appliance
CN	Common Name
N	Name
G	Given Name
S	Surname
I	Initials
T	Personal title
E	E-mail
E-mail	E-mail
SN	Serial number
D	Description
TCGID	[Siemens] Trusted Center Global ID

The attribute/value pairs must be of the form *attribute=value* and be separated by commas. For example: *C=US, ST=Illinois, L=Chicago, O=Secure Computing, OU=Sales, CN=SG580*. It must match exactly the Distinguished Name of the remote party's local certificate to successfully authenticate the tunnel. When making a certificate-based tunnel between SnapGear appliances, you can obtain the **Distinguished Name** of a remote device's Certificate from the **Details** column of the appropriate local certificate on the **Certificate Lists** tab of the **IPSec** page.

Tip: Copy and paste all but the **Valid from** information from the Certificate Lists page before you configure the tunnel.

For more information on using certificates with VPN, see "Certificate management" on page 420.

- 13 [[Conditional, if **x.509 Certificates** was selected for **Authentication**] Select the required local certificate to use to negotiate the tunnel from the **Local Certificate** list. This is the list of local certificates that have been uploaded for x.509 authentication. Select the required certificate to be used to negotiate the tunnel.
- 14 Click **Finish**. The tunnel is added to the **Tunnel List** pane, and the **Status** column indicates the current status of the tunnel.

Refreshing status of IPSec VPN tunnels

Use this procedure to refresh the status of your IPSec VPN tunnels.




- 1 From the **VPN** menu, click **IPSec**. The IPSec VPN Setup page appears.
- 2 In the **Tunnel List** pane, click **Refresh**. The **Status** column displays the refreshed status of your tunnels. To view details about the status, click the linked status text. For more information, see “IPSec status details overview” on page 384.

Viewing the status of an IPsec VPN tunnel

Be sure to refresh the status before clicking the Status link.

- 1 From the **VPN** menu, click **IPsec**. The IPsec VPN Setup page appears.
- 2 In the **Tunnel List** pane, click the linked status in the **Status** column.

Figure 281: IPsec status

Tunnel List			
Connection	Remote Party	Status	
 t	1.1.1.3	Negotiating Phase 1	 
<div> <div>Refresh</div> <div>Quick Setup</div> <div>Advanced</div> </div>			

- 3 The activated link displays data similar to that shown in Figure 282:

Figure 282: IPsec status details

IPsec	Certificate Lists
Interfaces Loaded	
000 interface ipsec0/eth1 10.10.57.200 pmtu=1500	
000 interface ipsec0/eth1 10.10.57.200 pmtu=1500	
Phase 2 Ciphers Loaded	
000 algorithm ESP encrypt: id=2, name=ESP_DES, ivlen=64, keysize=64, keysize=64	
000 algorithm ESP encrypt: id=3, name=ESP_3DES, ivlen=64, keysize=168, keysize=168	
000 algorithm ESP encrypt: id=12, name=ESP_AES, ivlen=128, keysize=128, keysize=128	
Phase 2 Hashes Loaded	
000 algorithm ESP auth attr: id=1, name=AUTH_ALGORITHM_HMAC_MD5, keysize=128, keysize=128	
000 algorithm ESP auth attr: id=2, name=AUTH_ALGORITHM_HMAC_SHA1, keysize=160, keysize=160	
Phase 1 Ciphers Loaded	
000 algorithm IKE encrypt: id=7, name=OAKLEY_AES_CBC, blocksize=16, keydeflen=128	
000 algorithm IKE encrypt: id=5, name=OAKLEY_3DES_CBC, blocksize=8, keydeflen=192	
000 algorithm IKE encrypt: id=1, name=OAKLEY_DES_CBC, blocksize=8, keydeflen=64	
Phase 1 Hashes Loaded	
000 algorithm IKE hash: id=2, name=OAKLEY_SHA, hashsize=20	
000 algorithm IKE hash: id=1, name=OAKLEY_MD5, hashsize=16	
Diffie Hellman Groups Loaded	
000 algorithm IKE dh group: id=1, name=OAKLEY_GROUP_MODP768, bits=768	
000 algorithm IKE dh group: id=2, name=OAKLEY_GROUP_MODP1024, bits=1024	
000 algorithm IKE dh group: id=5, name=OAKLEY_GROUP_MODP1536 (extension), bits=1536	
000 algorithm IKE dh group: id=42048, name=OAKLEY_GROUP_MODP2048 (extension), bits=2048	
000 algorithm IKE dh group: id=43072, name=OAKLEY_GROUP_MODP3072 (extension), bits=3072	
000 algorithm IKE dh group: id=44096, name=OAKLEY_GROUP_MODP4096 (extension), bits=4096	
Connection Details	
000 "n": 192.168.0.0/24===10.10.57.200---10.10.1.254...%any	
000 "n": ike life: 3600s; ipsec life: 3600s; rekey margin: 600s; rekey_fuzz: 100%	
000 "n": policy: PSK+ENCRYPT+TUNNEL+PFS; interface: eth1; unrouted	
000 "n": newest ISAKMP SA: #0; newest IPsec SA: #0; eroute owner: #0	
000 "n": IKE algorithms wanted: 5_000-2-2, flags=-strict	
000 "n": IKE algorithms found: 5_192-2_160-2,	
000 "n": ESP algorithms wanted: 3_000-2, ; pfs group=2; flags=-strict	
000 "n": ESP algorithms loaded: 3/168-2/160,	

- 4 When you are done viewing the information, click the **IPsec** tab to return to the main IPsec VPN Setup page. For details about the information displayed in the IPsec status page, see "IPsec status details overview" on page 384.

IPSec status details overview

This topic gives descriptions of the status sections shown in Figure 282 on page 383.

Interfaces Loaded — Lists the SnapGear appliance's interfaces that IPSec is using.

Phase 2 Ciphers Loaded — Lists the encryption ciphers that tunnels can be configured with for Phase 2 negotiations. This includes DES, 3DES, and AES.

Phase 2 Hashes Loaded — Lists the authentication hashes that tunnels can be configured with for Phase 2 negotiations. This includes MD5 and SHA1 (otherwise known as SHA).

Phase 1 Ciphers Loaded — Lists the encryption ciphers that tunnels can be configured with for Phase 1 negotiations. This includes DES, 3DES, and AES.

Phase 1 Hashes Loaded — Lists the authentication hashes that tunnels can be configured with for Phase 1 negotiations. This includes MD5 and SHA.

Diffie Hellman Groups Loaded — Lists the Diffie Hellman groups and Oakley group extensions that can be configured for both Phase 1 and Phase 2 negotiations.

Connection Details — Lists an overview of the tunnel's configuration. It contains the following information:

- An outline of the tunnel's network setup.
- Phase 1 and Phase 2 key lifetimes (**ike_life** and **IPSec_life** respectively).
- Type of keying.
- Type of authentication used. The **policy** line displays *PSK* for Preshared Key authentication. For RSA Digital Signatures or x.509 certificates, it displays *RSA*.
- If Perfect Forward Secrecy is enabled, the **policy** line has the *PFS* keyword. If PFS is disabled, the keyword does not appear.
- If IP Payload Compression is enabled, the **policy** line has *COMPRESS* keyword.
- The interface on which the tunnel is going out.
- The current Phase 1 key. This is the number that corresponds to the **newest ISAKMP SA** field. If phase 1 has not been successfully negotiated yet, there is no key.
- The current Phase 2 key. This is the number that corresponds to the **newest IPSec SA** field. If phase 1 has not been successfully negotiated yet, no Phase 2 key is shown.

- The Phase 1 proposal wanted. For example, if the line **IKE algorithms wanted** reads `5_000-2-2`:
 - `5_000` refers to cipher 3DES (where 3DES has an ID of 5, see “Phase 1 Ciphers Loaded” on page 384)
 - The first 2 in `5_000-2-2` refers to hash SHA (where SHA has an ID of 2, see “Phase 1 Hashes Loaded” on page 384)
 - The second 2 in `5_000-2-2` refers to the Diffie Hellman Group 2 (where Diffie Hellman Group 2 has an ID of 2).
- The Phase 2 proposal wanted. For example, if the line **ESP algorithms wanted** reads `3_000-2; pfs group=2`:
 - `3_000` refers to cipher 3DES (where 3DES has an ID of 3, see “Phase 1 Ciphers Loaded” on page 384)
 - The 2 in `3_000-2` refers to hash SHA1 or SHA (where SHA1 has an ID of 2, see “Phase 2 Hashes Loaded” on page 384)
 - `pfs group=2` refers to the Diffie Hellman Group 2 for Perfect Forward Secrecy where Diffie Hellman Group 2 has an ID of 2.

Negotiation State — Reports what stage of the negotiation process the tunnel is in. Once the Phase 1 has been successfully negotiated, the status displays *ISAKMP SA established*. Once the Phase 2 has been successfully negotiated, the status displays *IPSec SA established*. The tunnel is then established and running.

Disabling an IPsec VPN tunnel

Use this procedure to disable individual IPsec VPN tunnels.

- 1 From the **VPN** menu, click **IPsec**. The IPsec VPN Setup page appears.
- 2 In the **Tunnel List** pane, clear the enabled check box to the left of the tunnel. The check mark is no longer displayed, and the tunnel is disabled. To enable the tunnel again, select the enable check box.

Disabling IPsec VPN

Use this procedure to disable all IPsec VPN tunnels.

- 1 From the **VPN** menu, click **IPsec**. The IPsec VPN Setup page appears.
- 2 Clear the **Enable IPsec** check box.
- 3 Click **Submit**.

Deleting an IPsec VPN tunnel

- 1 From the **VPN** menu, click **IPsec**. The IPsec VPN Setup page appears.
- 2 In the Tunnel List page, select the delete icon for the tunnel you want to delete. You are prompted to confirm the delete.
- 3 Click **OK**.

IPSec Advanced Setup wizard

This topic contains example procedures for the various keying modes available in the IPSec advanced wizard.

Keying modes

The keying modes supported in the SnapGear appliance are Main, Aggressive, and Manual as described below:

- **Main** — The main mode has a more restrictive exchange for its key mode, which automatically exchanges encryption and authentication keys and protects the identities of the parties attempting to establish the tunnel. This mode is the most secure, but difficult to configure in environments where one end has a dynamic Internet IP address, or if one or both ends are behind NAT devices.

Aggressive — Has a less restrictive exchange that automatically exchanges encryption and authentication keys and uses less messages in the exchange when compared to main mode. Aggressive mode is typically used to allow parties that are configured with a dynamic IP address and a preshared secret to connect or if the SnapGear appliance or the remote party is behind a NAT device.

This mode is less secure than main mode, but much easier to configure in environments where one end has a dynamic Internet IP address. When using this mode, ensure to use a long and particularly difficult to guess pre-shared secret.

- **Manual** — Keys are manually defined; no keying exchange is required. Use this if you need to connect to a legacy device that does not support main or aggressive modes. Manual Keying requires the encryption and authentication keys to be explicitly specified by the user, and requires regular user intervention in the form of manual key changes. This method is considered less secure than automatic key exchange since it uses a static key.

Guidance procedures provided in this section include the following:

- “Main keying mode for an IPSec tunnel” on page 388
- “Aggressive keying mode for an IPSec tunnel” on page 401
- “Manual keying mode for an IPSec tunnel” on page 405

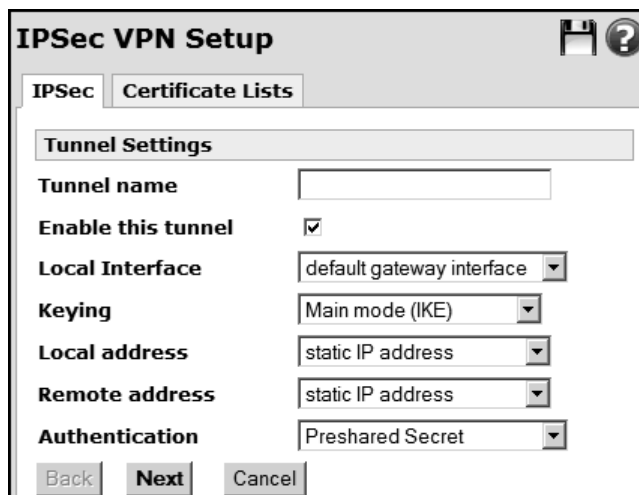
Main keying mode for an IPSec tunnel

Use this procedure as guidance for creating an IPSec tunnel using the Main mode (IKE) for keying. The configuration presented is a connection from static IP address to static IP address. At this time, IPSec VPN offloading only is supported for static IP addresses as the remote address. The example includes specifying an offload device.

This procedure also demonstrates how to set a next hop via the Local Interface Gateway field, which defines the default gateway assigned by an ISP.

- 1 From the **VPN** menu, click **IPSec**. The IPSec VPN Setup page appears.
- 2 Click **Advanced**. The Tunnel Settings page appears.

Figure 283: IPSec VPN Setup — Tunnel Settings page — Main keying



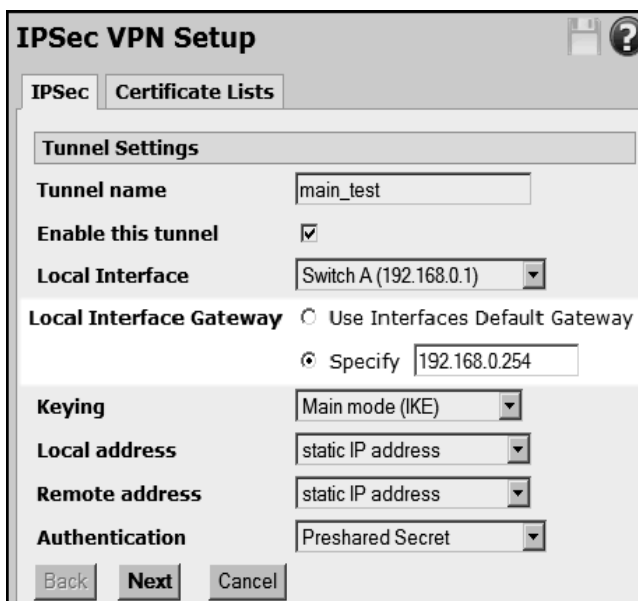
- a Enter a unique **Tunnel name**. This example uses `main_test`.
- b Leave the **Enable this tunnel** check box selected.
- c From the **Local Interface** list, select the interface the IPSec tunnel is to go out on. The options depend on what is currently configured on the appliance. For the vast majority of setups, the interface will be the **default gateway interface** to the Internet.

You may want to select an interface other than the default gateway when you have configured multiple Internet connections. If so, you must select something other than default gateway interface from the **Local Interface** list. When another entry is selected, the **Local Interface Gateway** field appears.

Note in Figure 284, **Switch A** is selected in the **Local Interface** list, rather than **default gateway interface**, so now you can indicate an option for the **Local Interface Gateway**. This is the next IP address (next hop) that IP packets are routed via to reach the remote endpoint after egress (exit) from the previously selected IPSec interface. Available options are:

- **Use Interfaces Default Gateway** — Uses the default gateway for the interface selected in the **Local Interface** list.
- **Specify** — Enter the IP address of the local gateway to use. This example uses 192.168.0.254.

Figure 284: Local Interface Gateway



The screenshot shows the 'IPSec VPN Setup' window with the 'Tunnel Settings' tab selected. The 'Local Interface' is 'Switch A (192.168.0.1)'. Under 'Local Interface Gateway', the 'Specify' radio button is selected with the IP address '192.168.0.254'. The 'Keying' is 'Main mode (IKE)'. The 'Local address', 'Remote address', and 'Authentication' are all set to 'static IP address', 'static IP address', and 'Preshared Secret' respectively. The 'Back', 'Next', and 'Cancel' buttons are at the bottom.

- Ensure the **Main mode (IKE)** is selected in the **Keying** list.
- Indicate the **Local address**, **Remote address**. This example uses static IP address.
- Select an authentication scheme from the **Authentication** list. Available options are:
 - Preshared Secret
 - RSA Digital Key Signature
 - x.509 Certificates

This examples uses Preshared Secret for authentication. For further information on available authentication schemes, refer to “Authenticat-ion” on page 376.

- 3 Click **Next**. The Local Endpoint Settings page appears. This page allows you to configure an IPSec tunnel's local endpoint settings. The options that display depend on your previous selections.

Figure 285: IPSec VPN
— Local Endpoint
Settings page

IPSec VPN Setup

IPSec **Certificate Lists**

Local Endpoint Settings

Tunnel name Main_test

Initiate Tunnel Negotiation ☒

Optional Endpoint ID

IP Payload Compression ☐

IPSec offload device None

Dead Peer Detection ☒

Delay (sec)

Timeout (sec)

Initiate Phase 1 & 2 rekeying ☒

- a If displayed, leave the **Initiate Tunnel Negotiation** check box selected. This causes the tunnel to start trying to negotiate a connection with the remote end immediately rather than waiting for the remote end of the connection to initiate a connection. Normally this setting, if displayed, should be enabled. This setting is not displayed if the remote end of the connection has a dynamic IP address.
- b Enter the applicable **Endpoint ID**:
 - **Optional Endpoint ID** [Conditional; appears if the tunnel has a static IP address and uses Preshared Secrets for authentication.] If left blank, defaults to the static IP address. This example has static IP addresses and uses preshared secrets, so Optional Endpoint ID is displayed. This example leaves the field blank and allows the default to the static IP address.
 - **Required Endpoint ID** [Conditional; required if the tunnel has a dynamic or DNS address; or if RSA digital signatures are used for authentication.] If the remote party is a SnapGear device, the ID must have the form *abcd@efgh*.
- c [Optional] To apply IPComp compression before encryption, select the **Payload compression** check box.
- d [Optional] To offload VPN connections to another SnapGear appliance, either select one from the current list of Definitions or click **New** and enter an IP address of the appliance in the **IPSec offload device** field.

For general information on VPN offloading, see “IPsec VPN offloading” on page 444. The allowed formats can be an IP address range of the following forms:

- a.b.c.d
- a.b.c.d-e
- a.b.c.d-e.f.g.h
- a.b.c.d/e
- a.b.c.d/e.f.g.h
- a.b.c.d+e

This example defines a new IP address for the offload device. Click **New** and enter 1 . 1 . 1 . 7.

Additional manual configuration is required. Refer to “Configuring for VPN offloading” on page 446.

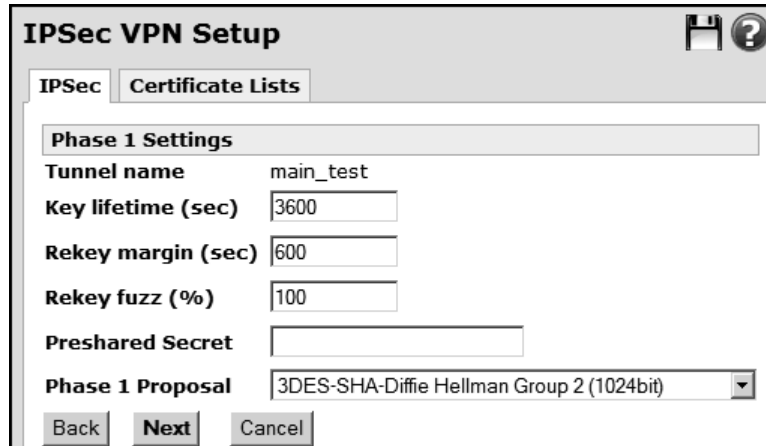
- e To allow the tunnel to be re-initiated if the remote party stops responding, select the **Dead Peer Detection** check box. The remote party must also support DPD (Dead Peer Detection).
 - Enter the number of seconds for delay in the **Delay** field. Default: 9.
 - Enter the number of seconds before timing out in the **Timeout** field. Default: 30.
 - f [Recommended] To enable automatic renegotiation of the tunnel when the keys are about to expire, select the **Initiate Phase 1 & 2 rekeying** check box.
- 4 Click **Next**. The Remote Endpoint Settings page appears.

Figure 286: IPsec VPN
— Remote Endpoint
Settings page — Main key
mode

The screenshot shows a window titled "IPsec VPN Setup" with a "Remote Endpoint Settings" tab selected. Inside the tab, there are three text input fields: "Tunnel name" with the value "main_test", "The remote party's IP address" with the value "2.4.6.8", and "Optional Endpoint ID" which is empty. At the bottom of the window are three buttons: "Back", "Next", and "Cancel".

- a Enter the IP address in the **remote party's IP address** field. This example uses 2 . 4 . 6 . 8.
 - b This example leaves the **Optional Endpoint ID** blank.
- 5 Click **Next**. The Phase 1 Settings page appears.

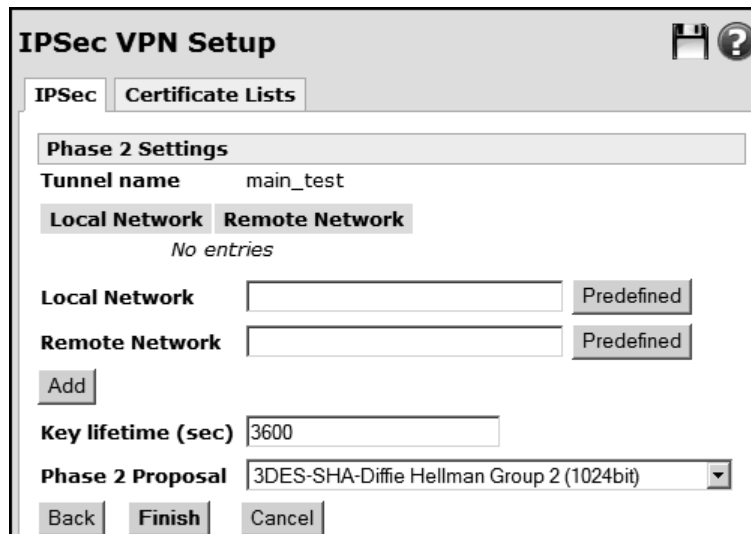
Figure 287: IPsec VPN
— Phase 1 Settings page



The screenshot shows the 'IPsec VPN Setup' window with the 'IPsec' tab selected. The 'Phase 1 Settings' section is active. The 'Tunnel name' is 'main_test'. The 'Key lifetime (sec)' is 3600, 'Rekey margin (sec)' is 600, and 'Rekey fuzz (%)' is 100. The 'Preshared Secret' field is empty. The 'Phase 1 Proposal' is set to '3DES-SHA-Diffie Hellman Group 2 (1024bit)'. At the bottom are 'Back', 'Next', and 'Cancel' buttons.

- a Allow all of the defaults for the **Key lifetime**, **Rekey margin**, and **Rekey fuzz** fields.
 - b Enter the **Preshared Secret**.
- 6 Click **Next**. The Phase 2 Settings page appears.

Figure 288: IPsec VPN
— Phase 2 Settings page



The screenshot shows the 'IPsec VPN Setup' window with the 'IPsec' tab selected. The 'Phase 2 Settings' section is active. The 'Tunnel name' is 'main_test'. Below it are 'Local Network' and 'Remote Network' sections, both currently empty with a 'No entries' message. Each has an 'Add' button and a 'Predefined' button. The 'Key lifetime (sec)' is 3600. The 'Phase 2 Proposal' is set to '3DES-SHA-Diffie Hellman Group 2 (1024bit)'. At the bottom are 'Back', 'Finish', and 'Cancel' buttons.

- 7 You must specify at least one Local and Remote network pair for the IPsec tunnel. If this is a host-to-host tunnel, you need to explicitly add the local and remote endpoint for the tunnel as a network pair.

- a Indicate the **Local Network** that will have access to the remote network. You can select from a list of predefined values based on the current network configuration and existing Definitions, or you can define custom networks. Custom networks can be specified in the following formats:
 - Can be left blank
 - Can be an IP address of the form a.b.c.d
 - An IP address and a valid netmask specified in either the /24 or 255.255.255.0 format
- b Indicate the **Remote Network** that the specified local network should have access to. You can select from a list of predefined values based on the current network configuration and existing Definitions, or you can define custom networks. Custom networks can be specified in the following formats:
 - Can be an IP address of the form a.b.c.d
 - An IP address and a valid netmask specified in either the /24 or 255.255.255.0 format
- c Click **Add**. The pair appears in the **Local and Remote Network** list. You can click the delete icon to delete the pair and define a different pair.

Note: You can add as many network pairs as required for your environment. The network pairs defined in this page define the traffic that IPSec passes over the tunnel. If the traffic does not match the network pairs defined in the Phase 2 Settings page, IPSec drops the packets.

Figure 289: Local Endpoint Settings

The screenshot shows the 'IPSec VPN Setup' window with the 'Phase 2 Settings' tab selected. The 'Tunnel name' is 'main_test'. Below it, there are two columns: 'Local Network' and 'Remote Network'. The 'Local Network' is set to 'Network of Switch A' and the 'Remote Network' is set to 'Remote Endpoint'. There is a delete icon to the right of the 'Remote Network' field. Below these fields, there is an 'Add' button. Further down, the 'Key lifetime (sec)' is set to '3600' and the 'Phase 2 Proposal' is set to '3DES-SHA-Diffie Hellman Group 2 (1024bit)'. At the bottom, there are 'Back', 'Finish', and 'Cancel' buttons.

- d [Optional] In the **Key lifetime** field, adjust the number of seconds between when the phase 2 keys should be renegotiated. Default: 3600.

- e Leave the **Allow the Phase 2 Proposal** at the default. The default setting is nearly always correct, particularly if you are communicating with another SnapGear appliance.
- 8 Click **Finish**. The tunnel is added to the **Tunnel List** pane, and the **Status** column indicates the current status of the tunnel.

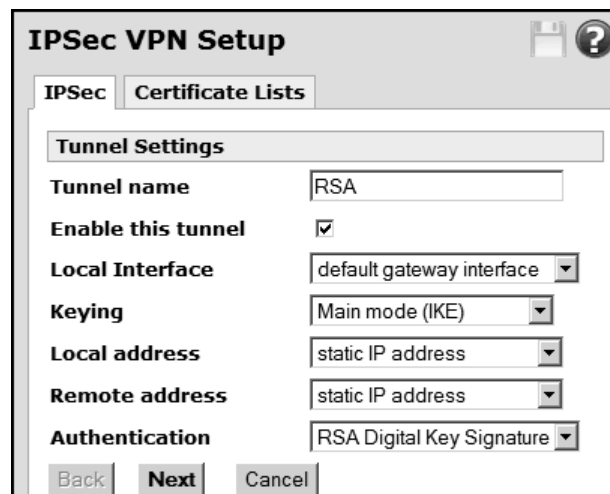
Setting up a tunnel with RSA signatures authentication

Use this procedure as guidance for configuring an IPsec VPN tunnel using RSA digital signatures for authentication.

This example assumes the remote appliance is also a SnapGear appliance, and both appliances have static IP addresses.

- 1 From the **VPN** menu, click **IPsec**. The IPsec VPN Setup page appears.
- 2 Click **Advanced**. The Tunnel Settings page appears.

Figure 290: IPsec VPN Setup — Tunnel Settings page — RSA authentication



- a Enter a unique **Tunnel name**. This example uses **RSA**.
- b Leave the **Enable this tunnel** check box selected.
- c From the **Local Interface** list, allow the **Local Interface** to default to the **default gateway interface** to the Internet.
- d Allow the **Local** and **Remote** addresses to default to **static IP address**.
- e From the **Authentication** list, select **RSA Digital Key Signature**.

- 3 Click **Next**. The Local Endpoint Settings page appears.

Figure 291: IPsec VPN Setup — Local Endpoint Settings page — RSA authentication

IPsec VPN Setup

IPsec Certificate Lists

Local Endpoint Settings

Tunnel name RSA

Initiate Tunnel Negotiation ☒

Required Endpoint ID local@corphead

IP Payload Compression ☐

IPsec offload device None

Dead Peer Detection ☒

Delay (sec) 9

Timeout (sec) 30

Initiate Phase 1 & 2 rekeying ☒

- a Leave the **Initiate Tunnel Negotiation** check box selected.
 - b Enter the applicable **Required Endpoint ID**. This example uses the SnapGear format and the value `local@corphead`.
 - c Allow the remainder of the fields to their defaults.
- 4 Click **Next**. The Remote Endpoint Settings page appears.

Figure 292: IPsec VPN Setup — Remote Endpoint Settings page — RSA authentication

IPsec VPN Setup

IPsec Certificate Lists

Remote Endpoint Settings

Tunnel name RSA

The remote party's IP address 1.1.1.3

Required Endpoint ID remote@branch

RSA key length 2048 bits

- a Enter the IP address of the remote party. This example uses `1.1.1.3`.
- b Enter the **Required Endpoint ID**. This example uses `remote@branch`.

- c Select an option for the **RSA key length**. This allows the device generated RSA public/private key pair to be specified when *configuring* a tunnel to use RSA Digital Signatures authentication. When *modifying* a tunnel using RSA Digital Signatures, this allows the option to modify the private part of the RSA key or leave the keys unchanged. Available options are:

- 512 bits
- 1024 bits
- 1536 bits
- 2048 bits
- Custom RSA key

Note: The greater the key pair length, the longer the time required to generate the keys. It may take up to 20 minutes to generate a 2048 bit RSA key.

- 5 Click **Next**. The Phase 1 Settings page appears.

Figure 293: IPsec VPN
— Phase 1 Settings page
(RSA)

The screenshot shows the 'IPsec VPN Setup' window with the 'Phase 1 Settings' tab selected. The 'IPsec' tab is also visible. The settings are as follows:

Field	Value
Tunnel name	RSA
Key lifetime (sec)	3600
Rekey margin (sec)	600
Rekey fuzz (%)	100
Local Public Key	HB2IUS2E97aAU1seVKob
Remote Public Key	HB2IUS2E97aAU1seVKob
Phase 1 Proposal	3DES-SHA-Diffie Hellman Group 2 (1024bit)

At the bottom, there are three buttons: 'Back', 'Next', and 'Cancel'.

- a Allow all of the defaults for the **Key lifetime**, **Rekey margin**, and **Rekey fuzz** fields.
- b Allow the **Local Public Key** to prepopulate. This field is automatically populated. It is used as the Remote Public Key of the remote party's tunnel configuration.
- c In the **Remote Public Key** field, enter the public part of the remote party's RSA Key generated for RSA Digital Key authentication. This field must be populated with the remote party's public RSA key.
- d Allow the **Phase 1 Proposal** field to default.
- 6 Click **Next**. The Phase 2 Settings page appears.

Figure 294: IPsec VPN
— Phase 2 Settings page
(RSA)

IPsec VPN Setup

IPsec Certificate Lists

Phase 2 Settings

Tunnel name RSA

Local Network Remote Network

No entries

Local Network Network of Switch A Custom

Remote Network Remote Endpoint Custom

Add

Key lifetime (sec) 3600

Phase 2 Proposal 3DES-SHA-Diffie Hellman Group 2 (1024bit)

Back Finish Cancel

- a For the **Local Network** field, this example selects the **Network of Switch A** from its Predefined values.
 - b The **Remote Endpoint** is selected for the **Remote Network**.
 - c Click **Add**. The pair appears in the **Local and Remote Network** list.
 - d Leave the **Key lifetime** field at the default value.
 - e Leave the **Allow the Phase 2 Proposal** at the default.
- 7 Click **Finish**. The tunnel is added to the **Tunnel List** pane, and the **Status** column indicates the current status of the tunnel.

Setting up a tunnel using x.509 certificates for authentication

This procedure steps through a basic configuration for using x.509 certificates for authenticating an IPSec VPN tunnel. This example assumes the remote appliance is a SnapGear appliance, and both appliances have static IP addresses. It also assumes you have uploaded your x.509 certificates. For instructions, refer to “Adding a certificate for use with IPSec VPN” on page 431. The root CA needs to be uploaded to both appliances. The local and remote certificates and keys must be uploaded to their respective appliances before you can establish an IPSec VPN tunnel.

- 1 From the **VPN** menu, click **IPSec**. The IPSec VPN Setup page appears.
- 2 Click **Advanced**. The Tunnel Settings page appears.

Figure 295: IPSec VPN Setup — Tunnel Settings page — RSA authentication

IPSec VPN Setup

IPSec **Certificate Lists**

Tunnel Settings

Tunnel name certs

Enable this tunnel ☒

Local Interface default gateway interface

Keying Main mode (IKE)

Local address static IP address

Remote address static IP address

Authentication x.509 Certificates

Back Next Cancel

- a Enter a unique **Tunnel name**. This example uses **certs**.
- b Leave the **Enable this tunnel** check box selected.
- c From the **Local Interface** list, allow the **Local Interface** to default to the **default gateway interface** to the Internet.
- d Allow the **Local** and **Remote** addresses to default to **static IP address**.
- e From the **Authentication** list, select **x.509 Certificates**.

- 3 Click **Next**. The Local Endpoint Settings page appears.

Figure 296: IPsec VPN Setup — Local Endpoint Settings page — x.509 authentication

- 4 Allow all of the fields to remain at their defaults. Click **Next**. The Remote Endpoint Settings page appears.

Figure 297: IPsec VPN Setup — Remote Endpoint Settings page — RSA authentication

- a Enter the IP address of the remote party. This example uses 1.1.1.3.
- b Enter the **Distinguished Name**. This example uses C=US, ST=MN, L=St. Paul, O=SecureComputing, CN=vpn.securecomputing.com, emailAddress=vpn@securecomputing.com

Tip: Copy the distinguished name from the Certificate Lists page.

- 5 Click **Next**. The Phase 1 Settings page appears. Note that the Local Certificate field displays.

Figure 298: IPsec VPN Setup — Remote Endpoint Settings page — RSA authentication

IPsec VPN Setup

IPsec Certificate Lists

Phase 1 Settings

Tunnel name certs

Key lifetime (sec) 3600

Rekey margin (sec) 600

Rekey fuzz (%) 100

Local Certificate headoffice.pem

Phase 1 Proposal 3DES-SHA-Diffie Hellman Group 2 (1024bit)

Back Next Cancel

- 6 Select the local certificate you want to use for authentication from the **Local Certificate** list.
- 7 Allow all of the other fields to remain at their defaults. Click **Next**. The Phase 2 Settings page appears.

Figure 299: IPsec VPN — Phase 2 Settings page (x.509)

IPsec VPN Setup

IPsec Certificate Lists

Phase 2 Settings

Tunnel name certs

Local Network Remote Network

Network of LAN 172.17.4.0/24

Local Network Predefined

Remote Network Predefined

Add

Key lifetime (sec) 3600

Phase 2 Proposal 3DES-SHA-Diffie Hellman Group 2 (1024bit)

Back Finish Cancel

- a Indicate the **Local Network** and **Remote Network** values. This examples uses the Predefined **Network of LAN** for **Local Network**, and **172.17.4.0/24** for the **Remote Network**. Click **Add**. The pair appears in the **Local and Remote Network** list.
- b Leave the **Key lifetime** field at the default value.

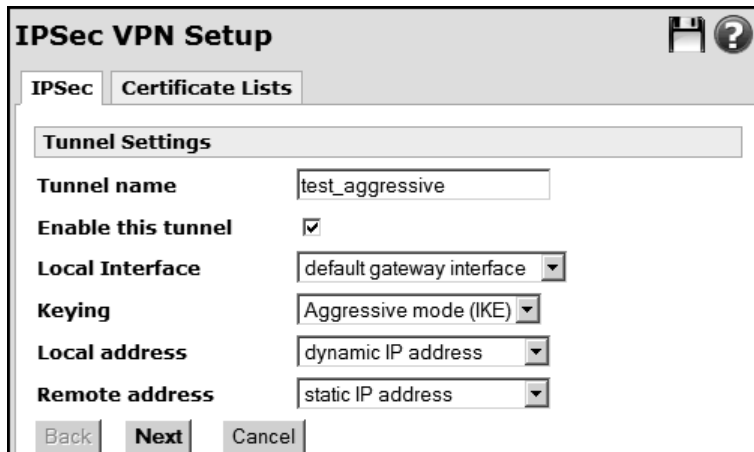
- c Leave the **Allow the Phase 2 Proposal** at the default.
- 8 Click **Finish**. The tunnel is added to the **Tunnel List** pane, and the **Status** column indicates the current status of the tunnel.

Aggressive keying mode for an IPsec tunnel

Use the aggressive mode for a less restrictive exchange of key mode. The example configuration presented in this procedure is a connection from a local dynamic IP address to a remote static IP address.

- 1 From the **VPN** menu, click **IPsec**. The IPsec VPN Setup page appears.
- 2 Click **Advanced**. The Tunnel Settings page appears.

Figure 300: Tunnel
Settings page —
Aggressive keying mode



- a Enter a unique **Tunnel name**. This example uses `test_aggressive`.
- b Leave the **Enable this tunnel** check box selected.
- c From the **Local Interface** list, select the interface the IPsec tunnel is to go out on. This example uses the **default gateway interface**.
- d Ensure you select **Aggressive mode (IKE)** from the **Keying** list.
- e Indicate the **Local address**. This example uses a **dynamic IP address**.
- f Indicate the **Remote address**. This example uses a **static IP address**.

3 Click **Next**. The Local Endpoint Settings page appears.

Figure 301: Local
Endpoint Settings —
Aggressive keying mode

The screenshot shows the 'Local Endpoint Settings' page of the 'IPSec VPN Setup' wizard. The 'IPSec' tab is selected. A warning message states: 'The interface that this IPSec tunnel is to go out on has been set as a **dynamic IP address**. There has been a previously configured tunnel(s) that has set this interface to use a **static IP address**. Please check the other tunnel configuration(s) to ensure they are configured as intended.' Below the warning, the 'Local Endpoint Settings' section contains the following fields: 'Tunnel name' (test_aggressive), 'Initiate Tunnel Negotiation' (checked), 'Required Endpoint ID' (empty text box), 'IP Payload Compression' (unchecked), 'IPSec offload device' (None with a 'New' button), 'Dead Peer Detection' (checked), 'Delay (sec)' (9), 'Timeout (sec)' (30), and 'Initiate Phase 1 & 2 rekeying' (checked). At the bottom are 'Back', 'Next', and 'Cancel' buttons.

4 Enter the **Required Endpoint ID**. This example uses `remote@au`. Leave the remainder of the fields at their default settings.

5 Click **Next**. The Remote Endpoint Settings page appears.

Figure 302: Local
Endpoint Settings —
Aggressive keying mode

The screenshot shows the 'Remote Endpoint Settings' page of the 'IPSec VPN Setup' wizard. The 'IPSec' tab is selected. The 'Remote Endpoint Settings' section contains the following fields: 'Tunnel name' (test_aggressive), 'The remote party's IP address' (empty text box), and 'Optional Endpoint ID' (empty text box). At the bottom are 'Back', 'Next', and 'Cancel' buttons.

- a Enter the IP address in the **remote party's IP address** field.
- b This example leaves the **Optional Endpoint ID** blank.

- 6 Click **Next**. The Phase 1 Settings page appears.

Figure 303: IPsec VPN
— Phase 1 Settings page

IPsec VPN Setup

IPsec Certificate Lists

Phase 1 Settings

Tunnel name test_aggressive

Key lifetime (sec) 3600

Rekey margin (sec) 600

Rekey fuzz (%) 100

Preshared Secret

Phase 1 Proposal 3DES-SHA-Diffie Hellman Group 2 (1024bit)

Back Next Cancel

- a Allow all of the defaults for the **Key lifetime**, **Rekey margin**, and **Rekey fuzz** fields.
 - b Enter the **Preshared Secret**.
- 7 Click **Next**. The Phase 2 Settings page appears.

Figure 304: IPsec VPN
— Phase 2 Settings page

IPsec VPN Setup

IPsec Certificate Lists

Phase 2 Settings

Tunnel name test_aggressive

Local Network Remote Network

No entries

Local Network Predefined

Remote Network Predefined

Add

Key lifetime (sec) 3600

Phase 2 Proposal 3DES-SHA-Diffie Hellman Group 2 (1024bit)

Back Finish Cancel

- 8 You must specify at least one Local and Remote network pair for the IPsec tunnel. If this is a host-to-host tunnel, you need to explicitly add the local and remote endpoint for the tunnel as a network pair.
- a Indicate the **Local Network** that will have access to the remote network. You can select from a list of predefined values based on the current

network configuration and existing Definitions, or you can define custom networks. Custom networks can be specified in the following formats:

- Can be left blank
- Can be an IP address of the form a.b.c.d
- An IP address and a valid netmask specified in either the /24 or 255.255.255.0 format

This example uses 1.1.1.3 for the custom local network.

- b** Indicate the **Remote Network** that the specified local network should have access to. You can select from a list of predefined values based on the current network configuration and existing Definitions, or you can define custom networks. Custom networks can be specified in the following formats:

- Can be an IP address of the form a.b.c.d
- An IP address and a valid netmask specified in either the /24 or 255.255.255.0 format

This example uses 3.3.3.3/32 for the custom remote network.

- c** [Conditional, for host-to-host tunnel] Click **Add**. The pair appears in the **Local and Remote Network** list. You can click the delete icon to delete the pair and define a different pair.

Figure 305: IPsec VPN
— Phase 2 Settings page

The screenshot shows the 'IPsec VPN Setup' window with the 'Phase 2 Settings' tab selected. The 'Tunnel name' is 'test_aggressive'. Below it, there are two columns: 'Local Network' and 'Remote Network'. The 'Local Network' column contains '1.1.1.3/32' and the 'Remote Network' column contains '3.3.3.3/32'. To the right of the 'Remote Network' entry is a delete icon. Below these columns are two input fields, one for 'Local Network' and one for 'Remote Network', each with a 'Predefined' button to its right. An 'Add' button is located below the 'Remote Network' input field. The 'Key lifetime (sec)' is set to '3600'. The 'Phase 2 Proposal' is set to '3DES-SHA-Diffie Hellman Group 2 (1024bit)'. At the bottom are 'Back', 'Finish', and 'Cancel' buttons.

- 9** Allow the remainder of the fields to remain at their default settings and click **Finish**. The tunnel is added to the **Tunnel List** pane, and the **Status** column indicates the current status of the tunnel.

Manual keying mode for an IPSec tunnel

Use this procedure as guidance for creating an IPSec tunnel using the manual mode for keying. This mode of keying is difficult to administer and troubleshoot and is not recommended unless you require access to a legacy device that does not support automatic keying modes.

- 1 From the **VPN** menu, click **IPSec**. The IPSec VPN Setup page appears.
- 2 Click **Advanced**. The Tunnel Settings page appears.

Figure 306: IPSec VPN Setup — Tunnel Settings page — Manual keying

The screenshot shows the 'IPSec VPN Setup' window with the 'Tunnel Settings' tab active. The 'Tunnel name' field is populated with 'Test_manual_key'. The 'Enable this tunnel' checkbox is checked. The 'Local Interface' dropdown is set to 'default gateway interface'. The 'Keying' dropdown is set to 'Manual'. Both 'Local address' and 'Remote address' dropdowns are set to 'static IP address'. The 'Next' button is highlighted.

- a Enter a name for the tunnel in **Tunnel name** field.
 - b Leave **Enable this tunnel** selected.
 - c Allow the **Local Interface** list to default to **default gateway interface**.
 - d From the **Keying** list, select **Manual**.
 - e Select a **Local** and **Remote address** from the lists. This example uses the default static IP address.
- 3 Click **Next**. The Local Endpoint Settings page appears. This page is where you configure an IPSec tunnel's local endpoint settings for manual keying.

Figure 307: IPsec VPN
Setup — Local Endpoint
Settings page

The image shows a screenshot of the 'IPsec VPN Setup' dialog box. The 'Local Endpoint Settings' tab is selected. The 'Tunnel name' field contains 't'. The 'SPI number' field contains '0x100'. The 'Authentication Key' field contains '0xb467b6c7bc934ff34a52f25'. The 'Encryption Key' field contains '0xc36068cfa2a2694dcd72d5'. The 'Cipher and Hash' dropdown menu is set to '3DES-MD5-96'. The 'Local Network' field is empty. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

Local Endpoint Settings	
Tunnel name	t
SPI number	0x100
Authentication Key	0xb467b6c7bc934ff34a52f25
Encryption Key	0xc36068cfa2a2694dcd72d5
Cipher and Hash	3DES-MD5-96
Local Network	

- a** Enter a unique, hexadecimal value for SPI (Security Parameter Index) in the **SPI** field. The SPI is used to establish and uniquely identify the tunnel, and determine which key is used to encrypt and decrypt the packets.
 - Format: *0xhex*, where *hex* is a three-digit hexadecimal number
 - Range: **0x100–0xfff**
- b** Enter an **Authentication Key**. The ESP Authentication Key. It must be of the form *0xhex*, where *hex* is one or more hexadecimal digits. The hex part must be exactly 32 characters long when using MD5 or 40 characters long when using SHA1 (excluding any underscore characters).
- c** Enter an **Encryption key**. The ESP Encryption Key. It must be of the form *0xhex*, where *hex* is one or more hexadecimal digits. The hex part must be exactly 16 characters long when using DES or 48 characters long when using 3DES (excluding any underscore characters).

- d Select a **Cipher and Hash** option. These are ESP encryption/authentication algorithms that you can use for the tunnel. The option selected must correspond to the encryption and authentication keys used. Available options are:
 - **3DES-MD5-96** uses the encryption transform following the Triple-DES standard in Cipher-Block-Chaining mode with authentication provided by HMAC and MD5 (96 bit authenticator). It uses a 192 bit 3DES encryption key and a 128 bit HMAC-MD5 authentication key.
 - **3DES-SHA1-96** uses the encryption transform following the Triple-DES standard in Cipher-Block-Chaining mode with authentication provided by HMAC and SHA1 (96 bit authenticator). It uses a 192 bit 3DES encryption key and a 160 bit HMAC-SHA1 authentication key.
 - **DES-MD5-96** uses the encryption transform following the DES standard in Cipher-Block_Chaining mode with authentication provided by HMAC and MD5 (96 bit authenticator). It uses a 56 bit DES encryption key and a 128 bit HMAC-MD5 authentication key.
 - **DES-SHA1-96** uses the encryption transform following the DES standard in Cipher-Block_Chaining mode with authentication provided by HMAC and SHA1 (96 bit authenticator). It uses a 56 bit DES encryption key and a 160 bit HMAC-SHA1 authentication key.
 - e [Optional] Enter an IP address and valid netmask in the **Local Network** field. This is the local network behind the appliance that the remote party accesses. Can be specified in either the /24 or 255.255.255.0 format.
- 4 Click **Next**. The Remote Endpoint Settings page appears. Use this page to to configure an IPSec tunnel's remote endpoint settings for manual keying.

Figure 308: Setup — Remote Endpoint Settings page — Manual key mode

IPSec VPN Setup

IPSec Certificate Lists

Remote Endpoint Settings

Tunnel name Test_manual_key

The remote party's IP address

SPI number

Authentication Key

Encryption Key

Remote Network

Back Finish Cancel

- a Enter the Internet IP address of the remote party's IPSec endpoint in the **Remote party IP address** field.

- b** Enter a unique, hexadecimal value for SPI (Security Parameter Index) in the **SPI** field.
 - Format: `0xhex`, where *hex* is a three-digit hexadecimal number
 - Range: `0x100–0xffff`
 - c** Enter the **Authentication Key** that applies to the remote party. It must be of the form `0xhex`, where *hex* is one or more hexadecimal digits. The hex part must be exactly 32 characters long when using MD5 or 40 characters long when using SHA1 (excluding any underscore characters). It must use the same hash as the appliance's authentication key.
 - d** Enter the **Encryption Key** that applies to the remote party. It must be of the form `0xhex`, where *hex* is one or more hexadecimal digits. The hex part must be exactly 16 characters long when using DES or 48 characters long when using 3DES (excluding any underscore characters). It must use the same hash as the appliance's encryption key.
 - e** [Optional] Enter an IP address and valid netmask in the **Remote Network** field. This is the remote network behind the remote party to which the local party can have access. Can be specified in either the `/24` or `255.255.255.0` format.
- 5** Click **Finish**. The tunnel is added to the **Tunnel List** pane.

Converting an IPSec tunnel configuration to the advanced format

Use **Convert to Advanced** to convert the tunnel's configuration from using the Quick Setup to using the Advanced format. Subsequent modifications of the tunnel's configuration are viewed using the Advanced format.

With the advanced format, you can take advantage of features such as VPN offloading, keying modes, RSA Digital Key Signatures, and phase 1 & 2 rekeying for automatic tunnel renegotiation for expiring keys.

Use this procedure for general guidance when navigating the conversion wizard. For information on specific settings, refer to the procedures within the Advanced Setup topics. See “IPSec Advanced Setup wizard” on page 387.

- 1** From the **VPN** menu, click **IPSec**. The IPSec VPN Setup page appears.
- 2** Click the edit icon for the tunnel you want to convert to advanced format. The Tunnel Settings page opens.

Figure 309: IPsec
Convert to Advanced

IPsec VPN Setup

IPsec Certificate Lists

Tunnel Settings

Tunnel name: t-quick

Enable this tunnel: ☒

The remote party's IP address: 22.22.22 [Predefined]

Local Network: Network of Switch A [Custom]

Remote Network: Remote Endpoint [Custom]

Authentication: Preshared Secret

Local Endpoint ID: sg@local.com

Remote Endpoint ID: sg@remote.com

Preshared Secret: secret

[Convert to Advanced] [Finish] [Cancel]

- 3 Click **Convert to Advanced**. You are prompted to confirm the conversion.

Note: Once you confirm the conversion is confirmed, you can no longer use the Quick Setup to view or modify the tunnel configuration.

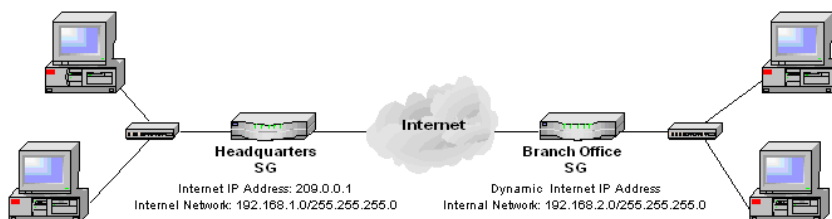
- 4 Click **OK**. The advanced wizard begins and the Tunnel Settings page appears.
- 5 Make your selections and click **Next**. The Local Endpoint Settings page appears.
- 6 Make your selections and click **Next**. The Remote Endpoint Settings page appears.
- 7 Make your selections and click **Next**. The Phase 1 Settings page appears.
- 8 Make your selections and click **Next**. The Phase 2 Settings page appears.
- 9 Click **Finish**.

IPSec example

SnapGear appliance to SnapGear appliance

There are many configurations possible when creating an IPSec tunnel. The most common and simplest is described in this topic. First the **Quick Setup** provides a one-page means to connect two sites together. For more control over the IPSec configuration, the **Advanced** configuration wizard provides additional fields. To connect two offices together, a network similar to the following is used.

Figure 310: Example SnapGear to Snapgear network



To route traffic between the Headquarters and Branch Office networks, an IPSec tunnel must be configured on both SnapGear appliances. This example steps through setting up the branch office, and then steps through setting up the headquarters for VPN.

Setting up the branch office

Step 1: Enabling IPSec VPN

- 1 From the **VPN** menu, click **IPSec**. The IPSec VPN Setup page appears.

Figure 311: IPSec General Settings

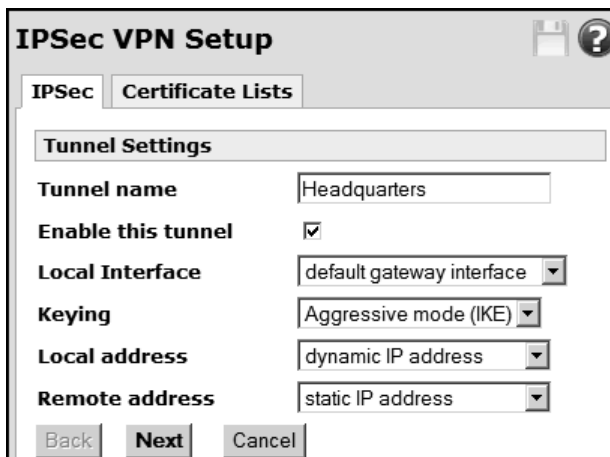
The screenshot shows the 'IPSec VPN Setup' web interface. At the top, there are two tabs: 'IPSec' (selected) and 'Certificate Lists'. Below the tabs is a section titled 'IPSec General Settings'. It contains a checkbox for 'Enable IPSec' which is currently unchecked, and a text input field for 'IPSec MTU'. Below these fields is a 'Submit' button. Underneath is a 'Tunnel List' section with a table header containing 'Connection', 'Remote Party', and 'Status'. The table body shows 'No entries'. At the bottom of the interface are three buttons: 'Refresh', 'Quick Setup', and 'Advanced'.

- 2 Select the **Enable IPSec** check box.
- 3 Click **Submit**.

Step 2: Configure a tunnel to connect to the headquarters office

- 1 Click **Advanced** under **Tunnel List**. The Tunnel Settings page appears.

Figure 312: IPSec VPN
Setup Tunnel Settings



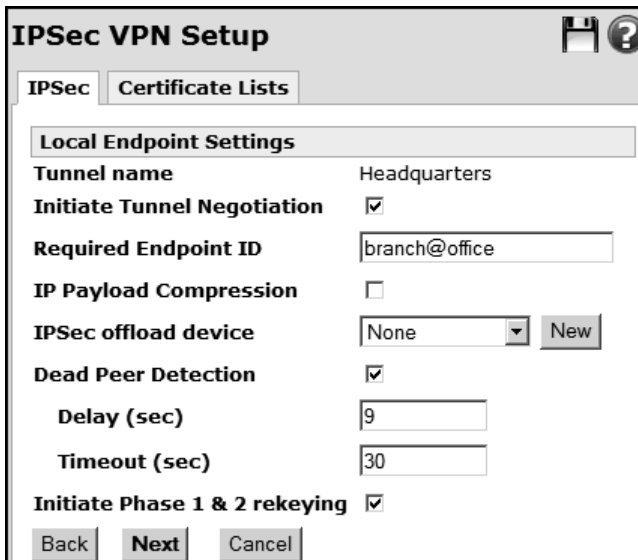
- 2 Fill in the **Tunnel name** field with a description for the tunnel. The name must not contain spaces or start with a number. In this example, enter *Headquarters*.
- 3 Leave the **Enable this tunnel** check box selected.
- 4 From the **Local Interface** list, select the interface the IPSec tunnel is to go out on. The options depend on what is currently configured on the SnapGear appliance. For the vast majority of setups, this is the **default gateway interface** to the Internet. In this example, leave the **default gateway interface** option selected.

***Note:** Select an interface other than the default gateway when you have more than one Internet connection or have configured aliased Internet interfaces, and require the IPSec tunnel to run on an interface other than the default gateway.*

- 5 From the **Keying** list, select the type of keying for the tunnel to use. In this example, select the **Aggressive Mode** option.
- 6 From the **Local address** list, select the type of IPSec endpoint this SnapGear appliance has on the interface on which the tunnel is going out. The SnapGear appliance can either have a **static IP**, **dynamic IP** or **DNS hostname address**. If a dynamic DNS service is to be used or there is a DNS hostname that resolves to the IP address of the port, then the DNS hostname address option should be selected. In this example, select **dynamic IP address**.
- 7 From the **Remote address** list, select the type of IPSec endpoint used by the remote party. In this example, select the **static IP address** option.
- 8 Click **Next** to configure the **Local Endpoint Settings**.

Step 4: Local endpoint settings

Figure 313: IPSec VPN
Setup Local Endpoint
Settings



The screenshot shows the 'IPSec VPN Setup' window with the 'Local Endpoint Settings' tab selected. The settings are as follows:

Setting	Value
Tunnel name	Headquarters
Initiate Tunnel Negotiation	<input checked="" type="checkbox"/>
Required Endpoint ID	branch@office
IP Payload Compression	<input type="checkbox"/>
IPSec offload device	None
Dead Peer Detection	<input checked="" type="checkbox"/>
Delay (sec)	9
Timeout (sec)	30
Initiate Phase 1 & 2 rekeying	<input checked="" type="checkbox"/>

At the bottom are buttons for 'Back', 'Next', and 'Cancel'.

- 1 Leave the **Initiate Tunnel Negotiation** check box selected.

Note: This option is not available when the SnapGear appliance has a static IP address and the remote party has a dynamic IP address.

- 2 Enter the **Required Endpoint ID** of the SnapGear appliance. In this example, enter: **branch@office**.

This ID is used to authenticate the SnapGear appliance to the remote party. It is optional if the tunnel has a static IP address and uses Preshared Secrets for authentication. If it is optional and the field is left blank, the **Endpoint ID** defaults to the static IP address. The Endpoint ID becomes required if the tunnel has a dynamic or DNS IP address or if RSA Digital Signatures are used for authentication.

If the remote party is a SnapGear appliance, the ID must have the form abcd@efgh. If the remote party is not a SnapGear appliance, refer the interoperability documents on the SnapGear Knowledge Base (<http://sgkb.securecomputing.com>) to determine what form it must take.

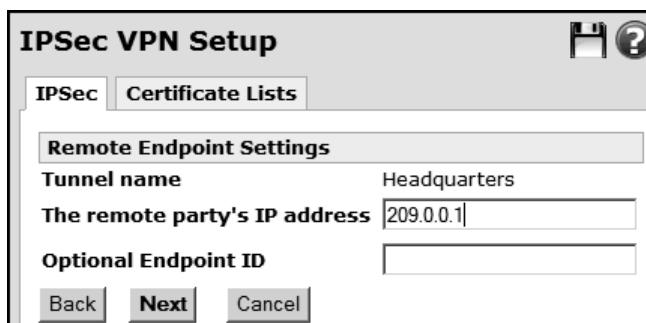
- 3 Leave the **IP Payload Compression** check box unselected.
- 4 Leave the **IPSec offload device** as **None**.
- 5 Select the **Dead Peer Detection** check box. This allows the tunnel to be restarted if the remote party stops responding. This option is only used if the remote party supports Dead Peer Detection. It operates by sending notifications and waiting for acknowledgements.
- 6 Enter the **Delay** and **Timeout** values for Dead Peer Detection. The default

times for the delay and timeout options are 9 and 30 seconds respectively. This means that a Dead Peer Detection notification is sent every 9 seconds (**Delay**) and if no response is received in 30 seconds (**Timeout**) then the SnapGear appliance attempts to restart the tunnel. In this example, leave the delay and timeout as their default values.

- 7 Leave the **Initiate Phase 1 & 2 rekeying** check box selected. This enables automatic renegotiation of the tunnel when the keys are about to expire.
- 8 Click **Next** to configure the **Remote Endpoint Settings**.

Step 5: Remote endpoint settings

Figure 314: IPSec VPN
Setup Remote Endpoint
Settings



The screenshot shows the 'IPSec VPN Setup' window with the 'Certificate Lists' tab selected. The 'Remote Endpoint Settings' section is active. It contains three fields: 'Tunnel name' with the value 'Headquarters', 'The remote party's IP address' with the value '209.0.0.1', and 'Optional Endpoint ID' which is empty. At the bottom are three buttons: 'Back', 'Next', and 'Cancel'.

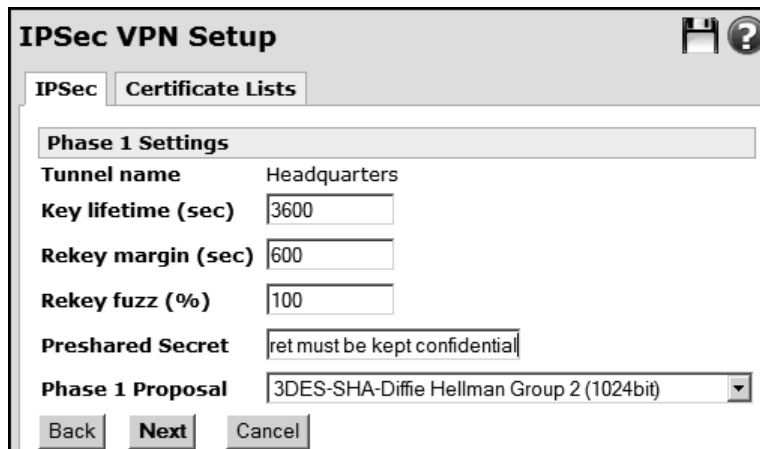
- 1 Enter the Internet IP address of the remote party in the **remote party's IP address** field. In this example, enter: **209.0.0.1**.
- 2 The **Optional Endpoint ID** is used to authenticate the remote party to the SnapGear appliance. For this example, leave the field blank.

The remote party's ID is optional if it has a static IP address and uses Pre-shared Secrets for authentication. It becomes a required field if the remote party has a dynamic IP or DNS hostname address or if RSA Digital Key Signatures are used for authentication. It is optional in this example, because the remote party has a static IP address. If the remote party is a SnapGear appliance, it must have the form *abcd@efgh*. If the remote party is not a SnapGear appliance, refer the interoperability documents on the SnapGear knowledgebase (<http://sgkb.securecomputing.com>) to determine what form it must take.

- 3 Click **Next** to configure the **Phase 1 Settings**.

Step 6: IPSec VPN Phase 1 settings

Figure 315: IPSec VPN
Setup Phase 1 Settings



The screenshot shows the 'IPSec VPN Setup' dialog box with the 'Phase 1 Settings' tab selected. The 'IPSec' tab is also visible. The settings are as follows:

Field	Value
Tunnel name	Headquarters
Key lifetime (sec)	3600
Rekey margin (sec)	600
Rekey fuzz (%)	100
Preshared Secret	ret must be kept confidential
Phase 1 Proposal	3DES-SHA-Diffie Hellman Group 2 (1024bit)

At the bottom are 'Back', 'Next', and 'Cancel' buttons.

- 1 In this example, leave the **Key Lifetime** as the default value of 3600 seconds.
Set the length of time before Phase 1 is renegotiated in the **Key lifetime (s)** field. The length may vary between 60 and 86400 minutes. Shorter values offer higher security at the expense of the computational overhead required to calculate new keys. For most applications 3600 seconds is recommended.
- 2 A new Phase 1 key can be renegotiated before the current one expires. The time for when this new key is negotiated before the current key expires can be set in the **Rekeymargin (s)** field. In this example, leave the **Rekeymargin** as the default value of 600 seconds.
- 3 The **Rekey fuzz** value refers to the maximum percentage by which the **Rekeymargin** should be randomly increased to randomize rekeying intervals. The **Key lifetimes** for both Phase 1 and Phase 2 are dependent on these values and must be greater than the value of "**Rekeymargin x (100 + Rekeyfuzz) / 100.**" In this example, leave the **Rekeyfuzz** as the default value of 100%.
- 4 Enter a secret in the **Preshared Secret** field. Keep a record of this secret as it is used to configure the remote party's secret. In this example, enter: **This secret must be kept confidential.**



Security Alert: The secret must be entered identically at each end of the tunnel. The tunnel fails to connect if the secret is not identical at both ends. The secret is a highly sensitive piece of information. It is essential to keep this information confidential. Communications over the IPSec tunnel may be compromised if this information is divulged.

- 5 Select a **Phase 1 Proposal**. In this example, select the **3DES-SHA-Diffie Hellman Group 2 (1024 bit)** option.

Any combination of the ciphers, hashes, and Diffie Hellman groups that the SnapGear appliance supports can be selected. The supported ciphers are *DES* (56 bits), *3DES* (168 bits) and *AES* (128, 196 and 256 bits). The supported hashes are *MD5* and *SHA* and the supported Diffie Hellman groups are 1 (768 bit), 2 (1024 bit) and 5 (1536 bits). The SnapGear appliance also supports extensions to the Diffie Hellman groups to include 2048, 3072 and 4096 bit Oakley groups.

- 6 Click **Next** to configure the **Phase 2 Settings**.

Step 6: IPSec VPN Phase 2 settings page

Figure 316: IPSec VPN
Setup Phase 2 Settings

- 1 Specify the **Local Network** and **Remote Network** to link together with the IPSec tunnel. For the **Local Network**, you can use a **Predefined** network, or enter a **Custom** network address. You must **Add** at least one local and one remote network.

Note: Only network traffic coming from a **Local Network** and destined for a **Remote Network** is allowed across the tunnel. IPSec uses its own routing mechanisms and disregards the main routing table.

- 2 For this example, select **Network of LAN** for the **Local Network**, and enter **192.168.1.0/24** for the **Remote Network** and click **Add**.
- 3 Set the length of time before Phase 2 is renegotiated in the **Key lifetime** field. The length may vary between 1 and 86400 seconds. For most applications 3600 seconds is recommended. In this example, leave the **Key Lifetime** as the default value of 3600 seconds.
- 4 Select a **Phase 2 Proposal**. Any combination of the ciphers, hashes, and Diffie Hellman groups that the SnapGear appliance supports can be

selected. The supported ciphers are *DES*, *3DES* and *AES* (128, 196 and 256 bits). The supported hashes are *MD5* and *SHA* and the supported Diffie Hellman group are 1 (768 bit), 2 (1024 bit) and 5 (1536 bits). The SnapGear appliance also supports extensions to the Diffie Hellman groups to include 2048, 3072 and 4096 bit Oakley groups. *Perfect Forward Secrecy* is enabled if a Diffie-Hellman group or an extension is chosen. Phase 2 can also have the option to not select a Diffie Hellman Group, in this case *Perfect Forward Secrecy* is not enabled. *Perfect Forward Secrecy* of keys provides greater security and is the recommended setting. In this example, select the **3DES-SHA-Diffie Hellman Group 2** (1024 bit) option.

- 5 Click **Finish** to save the tunnel configuration.

Configuring headquarters

This part of the example configures a tunnel to accept connections from the branch office. Many of the settings such as the **Preshared Secret**, **Phase 1** and **2 Proposals** and **Key Lifetimes** are the same as the branch office.

Step 1: Enable IPSec

- 1 From the **VPN** menu, click **IPSec**.
- 2 Select the **Enable IPSec** check box.
- 3 Select the type of IPSec endpoint the SnapGear appliance has on its Internet interface. In this example, select **static IP address**.
- 4 Leave the **IPSec MTU** unchanged.
- 5 Click **Submit**.
- 6 Click **Advanced**. The Tunnel Settings page appears.

Step 3: Complete the Tunnel settings page

- 1 Enter a description of the tunnel in the **Tunnel name** field. The name must not contain spaces or start or end with a number. In this example, enter: **Branch_Office**.
- 2 Leave the **Enable this tunnel** check box selected.
- 3 Select the Internet interface the IPSec tunnel is to go out on. In this example, select **default gateway interface** option.
- 4 Select the type of keying for the tunnel to use. In this example, select the **Aggressive mode (IKE)** option.
- 5 Select the type of IPSec endpoint this SnapGear appliance has. In this example, select the **static IP address** option in the **Local address** list.
- 6 Select the type of IPSec endpoint the remote party has. In this example, select the **dynamic IP address** option in the **Remote address** list.
- 7 Click **Next** to configure the **Local Endpoint Settings**.

Step 4: Local endpoint settings page

- 1 Leave the **Optional Endpoint ID** field blank in this example. It is optional because this SnapGear appliance has a static IP address. If the remote party is a SnapGear appliance and an Endpoint ID is used, it must have the form *abcd@efgh*. If the remote party is not a SnapGear appliance, refer to the interoperability documents on the SnapGear knowledgebase to determine what form it must take:
<http://sgkb.securecomputing.com>
- 2 Leave the **Enable IP Payload Compression** check box unselected.
- 3 Leave the **Enable Phase 1 & 2 rekeying to be initiated from my end** check box selected.
- 4 Click **Next** to configure the **Remote Endpoint Settings**.

Step 5: Remote endpoint settings page

- 1 Enter the **Required Endpoint ID** of the remote party. In this example, enter the **Local Endpoint ID** at the Branch Office which was: **branch@office**.
- 2 Click **Next** to configure the **Phase 1 Settings**.

Step 6: Phase 1 settings page

- 1 Set the length of time before Phase 1 is renegotiated in the **Key lifetime (s)** field. In this example, leave the **Key Lifetime** as the default value of 3600 minutes.
- 2 Set the time for when the new key is negotiated before the current key expires in the **Rekeymargin** field. In this example, leave the **Rekeymargin** as the default value of 600 seconds.
- 3 Set the maximum percentage by which the **Rekeymargin** should be randomly increased to randomize rekeying intervals in the **Rekeyfuzz** field. The **Key lifetimes** for both Phase 1 and Phase 2 are dependent on these values and must be greater than the value of "**Rekeymargin x (100 + Rekeyfuzz) / 100**." In this example, leave the **Rekeyfuzz** as the default value of 100%.
- 4 Enter a secret in the **Preshared Secret** field. This must remain confidential. In this example, enter the Preshared Secret used at the branch office SnapGear appliance, which was: **This secret must be kept confidential**.
- 5 Select a **Phase 1 Proposal**. In this example, select the **3DES-SHA-Diffie Hellman Group 2 (1024 bit)** option (same as the Branch Office **Phase 1 Proposal**).
- 6 Click **Next** to configure the **Phase 2 Settings**.

Step 7: Phase 2 settings page

- 1 Select **Network of LAN (Switch A)** for the **Local Network**, enter **192.168.2.0/24** for the **Remote Network** and click **Add**.
- 2 Set the length of time before Phase 2 is renegotiated in the **Key lifetime (s)** field. In this example, leave the **Key Lifetime** as the default value of 3600 seconds.
- 3 Select a **Phase 2 Proposal**. In this example, select the **3DES-SHA-Diffie Hellman Group 2 (1024 bit)** option (same as the Branch Office **Phase 2 Proposal**).
- 4 Click **Finish** to save the tunnel configuration. Once a tunnel has been configured, an entry with the tunnel name in the **Connection** column is shown. Click the status link to view the details for the tunnel.

NAT traversal support

NAT Traversal allows tunnels to be established when the IPSec endpoints reside behind NAT devices by encapsulating the ESP packets inside a UDP packet on port 4500. If any NAT devices are detected, the NAT Traversal feature is automatically used. It cannot be configured manually on the SnapGear appliance.

Dynamic DNS support

Internet Service Providers generally charge higher fees for static IP addresses than for dynamic IP addresses when connecting to the Internet. The SnapGear appliance can reduce costs since it allows tunnels to be established with both IPSec endpoints having dynamic IP addresses. The two endpoints must, however, be SnapGear appliances and at least one end must have dynamic DNS enabled. The SnapGear appliance supports a number of dynamic DNS providers. For information on configuring DNS, see “DNS” on page 153.

When configuring the tunnel, select the **DNS hostname address** type for the IPSec endpoint that has dynamic DNS supported and enable **Dead Peer Detection**. If the IP address of the SnapGear appliance’s DNS hostname changes, the tunnel automatically renegotiates and establishes the tunnel.

Certificate management

x.509 certificates can be used to authenticate IPSec endpoints during tunnel negotiation for Automatic Keying. The other methods are *Preshared Secrets* and *RSA Digital Signatures*.

Certificates need to be uploaded to the SnapGear appliance before they can be used in a tunnel. Certificates have time durations in which they are valid. Ensure that the certificates uploaded are valid and that the Date and Time settings have been set correctly on the SnapGear appliance.

The SnapGear appliance only supports certificates in *base64 PEM* or *binary DER* format. Some certificate authorities (CA) distribute certificates in a *PKCS12* format file. This format combines the CA certificate, local public certificate, and local private key certificate into one file. These certificates must be extracted before uploading them to the appliance; see “Extracting a PKCS12 certificate” on page 420 for instructions.

If you do not have access to certificates issued by a certificate authority (CA), you may create self-signed certificates; see “Creating a self-signed certificate” on page 421.

The OpenSSL application

The remainder of this section requires the OpenSSL application, run from a Windows command prompt (**Start > Run > type cmd**) or Linux shell prompt.

A Windows version of OpenSSL is provided in the *openss/* directory of the SG CD. Ensure that this directory is in your execution path, or copy all files from this directory into a working directory on your hard drive.

For operating systems other than Windows, OpenSSL is available for free download at:

<http://www.openssl.org/>

Extracting a PKCS12 certificate

Use this procedure to extract a certificate in PKCS12 format so it can be used on the SnapGear appliance.

To extract the CA certificate, run:

```
openssl pkcs12 -nomacver -cacerts -nokeys -in pkcs12_file  
-out ca_certificate.pem
```

.. where **pkcs12_file** is the PKCS12 file issued by the CA and **ca_certificate.pem** is the CA certificate to be uploaded into the SnapGear appliance.

When the application prompts you to **Enter Import Password**, enter the password used to create the certificate. If none was used simply press enter.

To extract the local public key certificate type, enter the following at the Windows command prompt:

```
openssl pkcs12 -nomacver -clcerts -nokeys -in pkcs12_file  
-out local_certificate.pem
```

.. where **pkcs12_file** is the PKCS12 file issued by the CA and
local_certificate.pem is the local public key certificate to be uploaded into the SnapGear appliance.

When the application prompts you to **Enter Import Password**, enter the password used to create the certificate. If none was used simply press enter.

To extract the local private key certificate type, enter the following at the Windows command prompt:

```
openssl pkcs12 -nomacver -nocerts -in pkcs12_file -out  
local_private_key.pem
```

.. where **pkcs12_file** is the PKCS12 file issued by the CA and
local_private_key.pem is the local private key certificate to be uploaded into the SnapGear appliance.

When the application prompts you to **Enter Import Password**, enter the password used to create the certificate. If none was used simply press enter. When the application prompts you to **Enter PEM pass phrase**, choose a secure pass phrase that is greater than 4 characters long. This is the pass phrase used to secure the private key file, and is the same pass phrase you enter when uploading the private key certificate into the SnapGear appliance. Verify the pass phrase by typing it in again.

The SnapGear appliance also supports *Certificate Revocation List* (CRL) files. A CRL is a list of certificates that have been revoked by the CA before they have expired. This may be necessary if the private key certificate has been compromised or if the holder of the certificate is to be denied the ability to establish a tunnel to the SnapGear appliance.

Creating a self-signed certificate

There are two steps to create a self-signed certificates: First, create a single CA certificate; second, create one or more local certificate pairs and sign them with the CA certificate.

Step 1: Creating a CA certificate

- 1 Create the CA directory:

```
mkdir rootCA
```

- 2 Create the serial number for the first certificate:

```
echo 01 > rootCA/serial
```

- 3 Create an empty CA database file under Windows:

```
type nul > rootCA/index.txt
```

.. or under Linux:

```
touch rootCA/index.txt
```

- 4 Create the CA certificate, omit the **-nodes** option if you want to use a password to secure the CA key:

```
openssl req -config openssl.cnf -new -x509 -keyout  
rootCA/ca.key -out rootCA/ca.pem -days DAYS_VALID -nodes
```

.. where *DAYS_VALID* is the number of days for which the root CA is valid.

Step 2: Creating local certificate pairs

For each local certificate you want to create, there are two steps.

First, create the certificate request:

```
openssl req -config openssl.cnf -new -keyout cert1.key -  
out cert1.req
```

Enter a PEM pass phrase, which is the same pass phrase required when you upload the key to the SnapGear appliance, and then enter the certificate details. All but the **Common Name** are optional and can be omitted.

Second, sign the certificate request with the CA:

```
openssl ca -config openssl.cnf -out cert1.pem -notext -  
infile cert1.req
```

You now have a local certificate pair, the local public certificate *cert1.pem* and the local private key certificate *cert1.key*, ready to use in the SnapGear appliance.

For each certificate required, change the *cert1.** filenames referenced in the above syntax as appropriate.

Using certificates with Windows IPsec

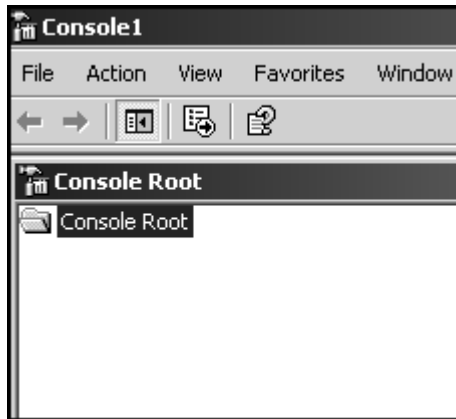
To create certificates to use with IPsec on a Windows system, first follow the previous instructions to create a CA certificate and local certificate pairs in “Creating a self-signed certificate” on page 421.

Windows IPsec requires the certificates to be in a PKCS12 format file. This format combines the CA certificate, local public certificate, and local private key certificate into one file.

```
openssl pkcs12 -export -inkey cert1.key -in cert1.pem -  
certfile rootCA/ca.pem -out cert1.p12 -name "Certificate  
1"
```

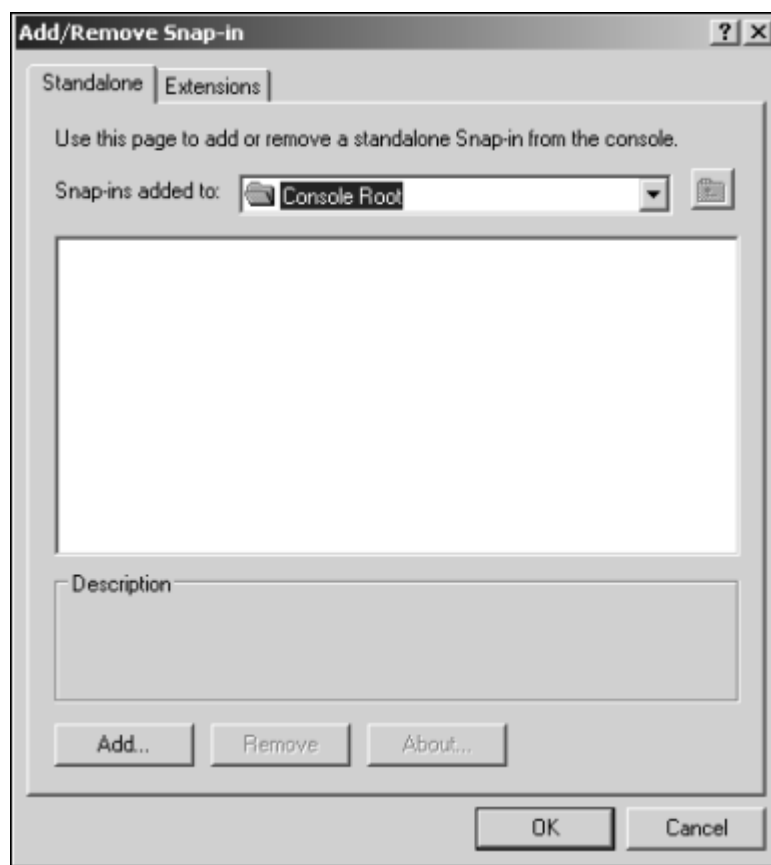
- 1 To install the new PCKS12 file, *cert1.p12*, on Windows XP, open up the *Microsoft Management Console* (**Start > Run >** then type **mmc**). The Certificate console opens.

Figure 317: MMC



- 2 Add the *Certificate Snap-in* (**File > Add/Remove Snap-in**). The Add/Remove Snap-in dialog box appears.

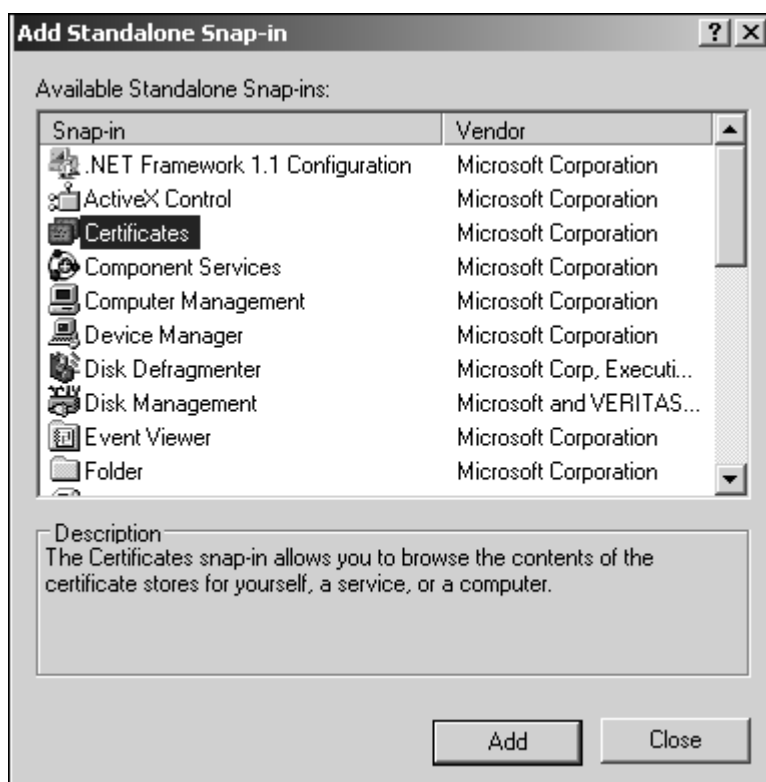
Figure 318: Snap-in



3 Click **Add**.

The Add Standalone Snap-in dialog box is displayed.

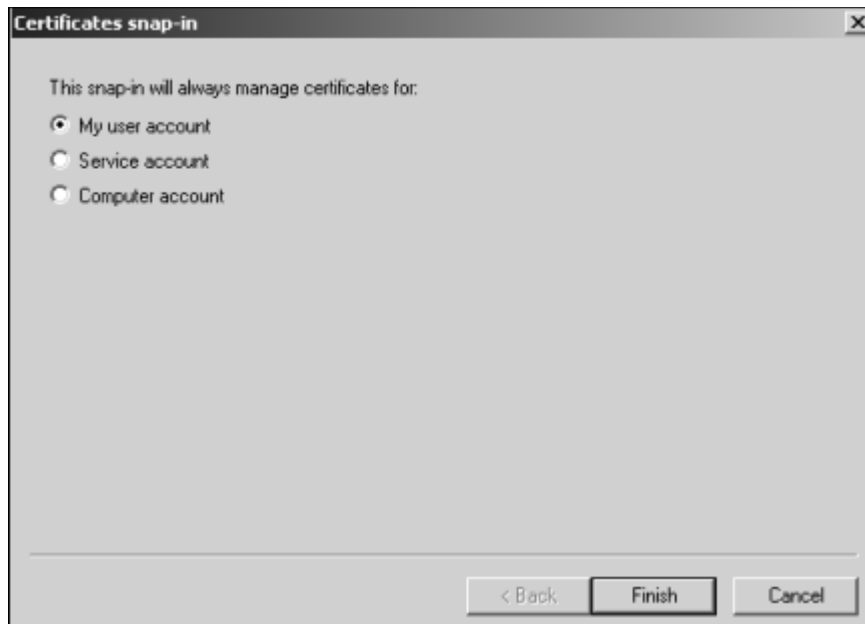
Figure 319: Add Standalone Snap-in



- 4 Select **Certificates** and click **Add**.

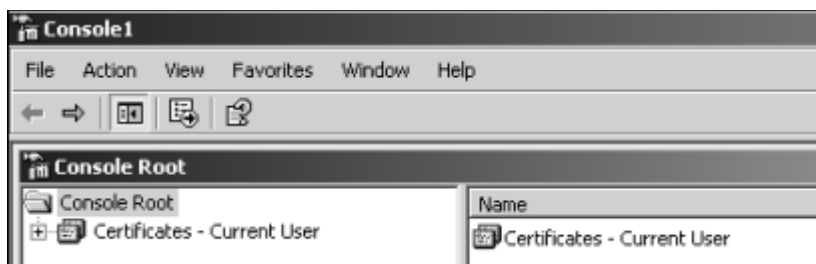
The Certificates snap-in dialog box is displayed.

Figure 320: Add
Standalone Snap-in



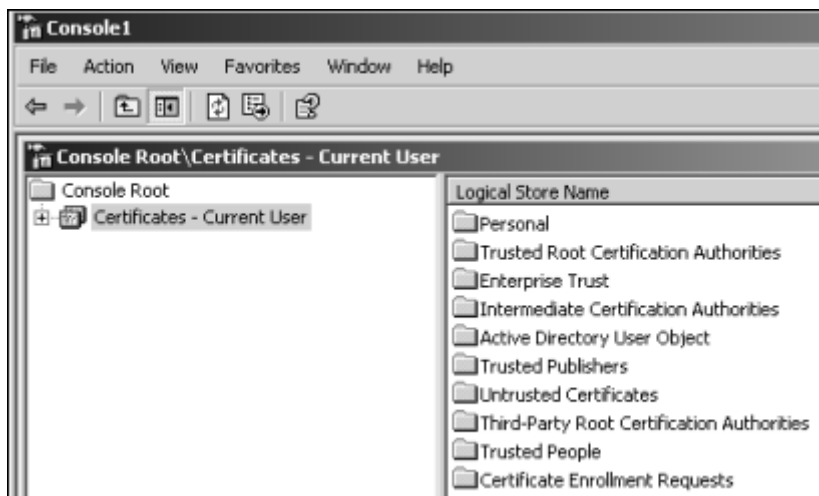
- 5 Select the account level you want the certificates installed for and click **Finish**. Click **Close** and **OK**.
- 6 Double-click **Certificates** to open the store.

Figure 321: Certificates
- Current User



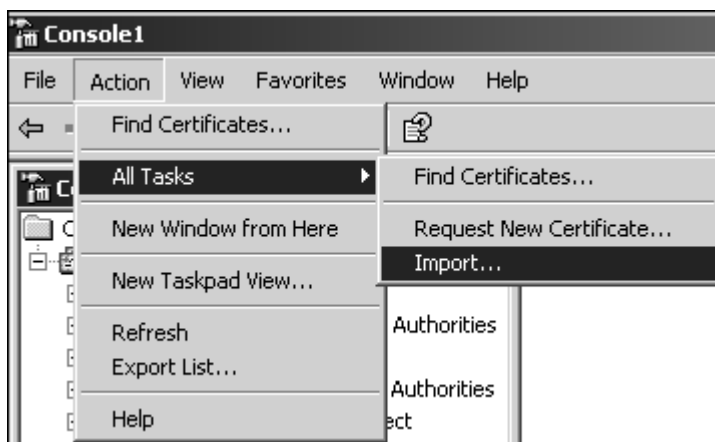
- 7 In the **Logical Store Name** pane, select the **Personal** store.

Figure 322: Logical
Store Name pane



- 8 To import a new certificate, click **Action > All Tasks > Import**.

Figure 323: Action menu



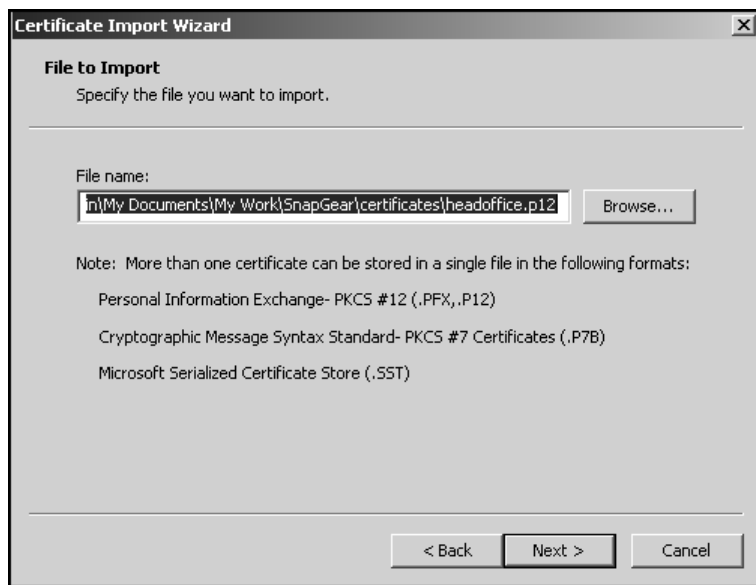
- 9 The Certificate Import wizard starts.

Figure 324: Certificate Import Wizard — Welcome page



10 Click **Next**. The File to Import wizard page is displayed.

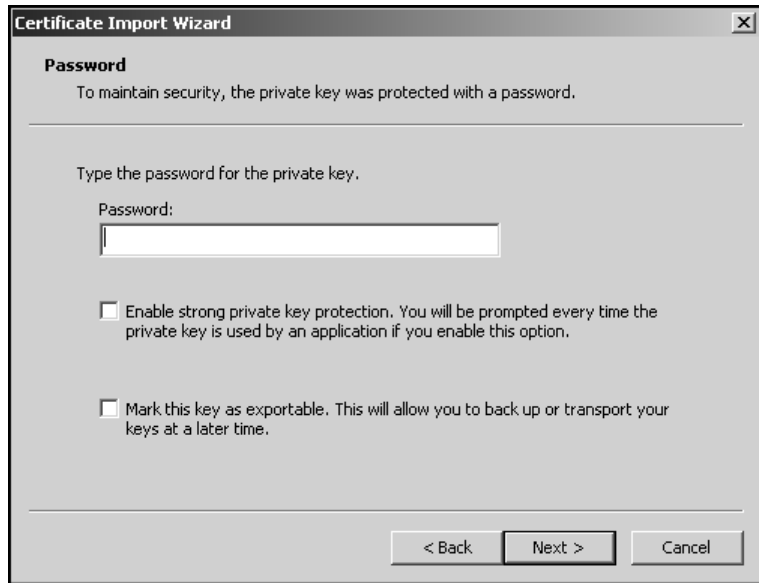
Figure 325: Certificate Import Wizard — File to Import page



11 Click **Browse** and locate your *cert1.p12*.

12 Click **Next**. The Password page appears.

Figure 326: Certificate Import Wizard — Password



13 Type in the **Export Password** if you used one.

14 Click **Next**. The Certificate Store page appears.

Figure 327: Certificate Import Wizard — Certificate Store page



15 Select the **Automatically select the certificate store based on the type of certificate** option.

16 Click **Next**. The Completing the Certificate Import Wizard page appears.

Figure 328: Certificate Import Wizard — Completion page



17 Click **Finish**.

Adding a certificate for use with IPsec VPN

The following types of certificates can be installed for use with IPsec VPN:

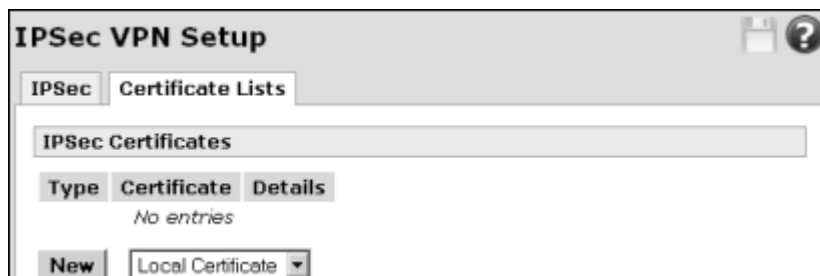
- **Local Certificate** is a private and public key pair signed by a trusted certificate authority. The certificate authority is used to establish that this device is trusted. The public key of the Certificate Authority of a public/private key pair must be known to the remote end of an IPsec connection.
- **CA Certificate** is the public key of a certificate authority. It is used to verify that a remote devices public key certificate is trusted.
- **CRL (Certificate Revocation Lists) Certificate** is a list of certificates no longer trusted by a certificate authority.

Adding a local certificate

Use this procedure to add a local certificate for IPsec VPN. The certificate must be in PEM or DER format.

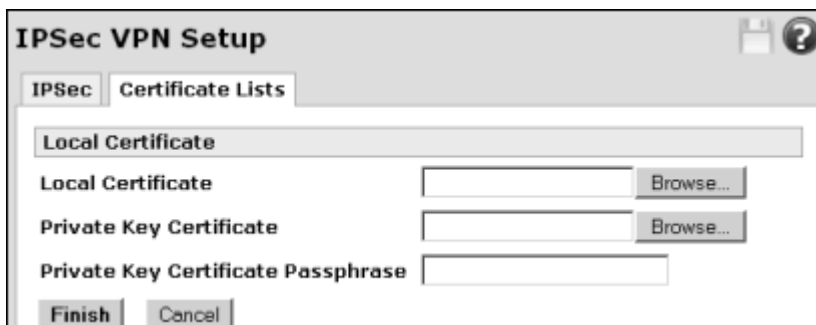
- 1 From the **VPN** menu, click **IPsec > Certificate Lists** tab. The IPsec Certificates page appears.

Figure 329: IPsec VPN
Local Certificate



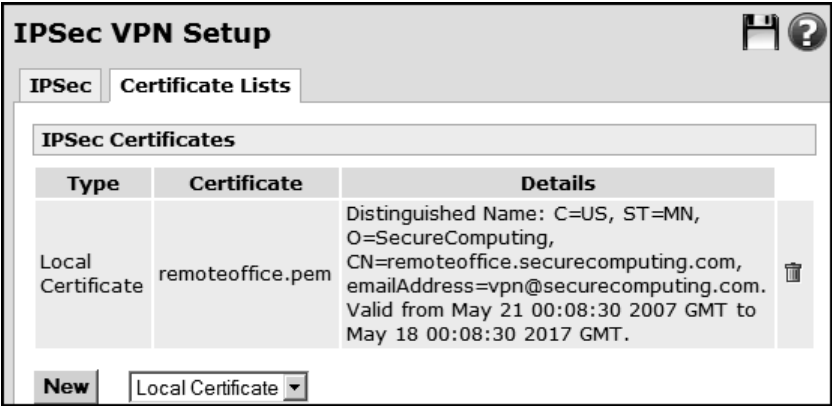
- 2 Select **Local Certificate** from the certificates list and click **New**. The Local Certificate page appears.

Figure 330: IPsec VPN
Local Certificate



- 3 Enter the Public Key certificate in the **Local Certificate** field. Click **Browse** to locate the file.
- 4 Enter the Local Private Key certificate in **Private Key Certificate** field.
- 5 Enter the passphrase to unlock the private key certificate in the **Private Key Certificate Passphrase** field.
- 6 Click **Finish**. The certificate is displayed in the list of installed certificates.

Figure 331: Installed IPsec VPN Certificates



The **Details** column shows the Distinguished Name of the certificate. This is needed for the Distinguished Name field of the Remote Endpoint Settings of the other end of a certificate-based IPsec tunnel.

Adding a CA certificate

Use this procedure to add a CA certificate for use with IPsec VPN. If a Certificate Authority is being used for authenticating IPsec connections, the Certificate Authority's public key certificate must be installed. The certificate must be in PEM or DER format.

- 1 From the **VPN** menu, click **IPsec > Certificate Lists** tab. The IPsec Certificates page appears.
- 2 Select **CA Certificate** from the certificates list and click **New**. The CA Certificate page appears.

Figure 332: IPsec VPN CA Certificate



- 3 Click **Browse** to locate the file.
- 4 Click **Finish**. The certificate is displayed in the list of installed certificates.

Figure 333: Installed
IPSec VPN Certificates



Adding a CRL certificate

Use this procedure to add a CRL certificate for use with IPsec VPN. The certificate must be in PEM or DER format.

- 1 From the **VPN** menu, click **IPSec > Certificate Lists** tab. The IPsec Certificates page appears.
- 2 Select **CRL** from the certificates list and click **New**. The CRL Certificate page appears.

Figure 334: IPsec VPN
CRL Certificate



- 3 Click **Browse** to locate the certificate.
- 4 Click **Finish**.

Deleting a certificate for IPsec VPN

Use this procedure to delete an installed certificate used for IPsec VPN.

- 1 From the **VPN** menu, click **IPSec > Certificate Lists** tab. The IPsec Certificates page appears.
- 2 Click the delete icon next to the certificate you want to delete.
- 3 You are prompted to confirm the delete. Click **OK**.

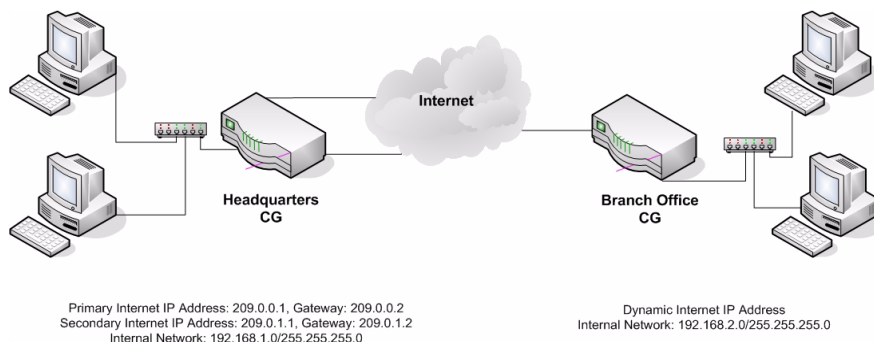
IPSec failover

Note: IPSec failover is applicable to the following models only: SG560, SG565, SG580, and SG720.

The SnapGear appliance can be configured to failover and fall forward between IPSec connections. Two common scenarios are described below.

The following scenario assumes that the Headquarters SG has two static Internet IP addresses and the Branch Office SG has a dynamic Internet IP address. The Branch Office SG establishes an IPSec tunnel to the primary Internet IP address at the Headquarters SG as the primary IPSec tunnel path. If this IPSec connection is detected to have failed, a failover IPSec tunnel is established to the secondary Internet IP address at the Headquarters SG. Once in the failover state, the Branch Office SG periodically determines if the primary IPSec tunnel path is functioning again, and if so, falls forward to use the primary link instead.

Figure 335: Example IPSec failover network



Setup an IPSec tunnel between the primary Internet IP Addresses (192.168.1.0/24 - 209.0.0.1 <> 210.0.0.1 – 192.168.2.0/24). Default values are used in the configuration unless otherwise specified below:

Headquarters SG configuration:

Tunnel name: PrimaryLink
Local interface: Internet port
Keying: Aggressive mode (IKE)
Local address: Static IP address
Remote address: Dynamic IP address
Local Interface Gateway: Internet port's gateway
Remote required endpoint ID: primary@branch
Local network: 192.168.1.0/255.255.255.0
Remote network: 192.168.2.0/255.255.255.0

Branch office SG configuration:

Tunnel name: PrimaryLink
Enable this tunnel: Unchecked
Local interface: Default gateway interface
Keying: Aggressive mode (IKE)
Local optional endpoint ID: primary@branch
The remote party's IP address: 209.0.0.1
Local network: 192.168.2.0/255.255.255.0
Remote network: 192.168.1.0/255.255.255.0

Setup an IPSec tunnel between the secondary Internet IP Addresses (192.168.1.0/24 - 209.0.1.1 <> 210.0.1.1 – 192.168.2.0/24). Default values are used in the configuration unless otherwise specified below:

Headquarters SG configuration:

Tunnel name: SecondaryLink
Local interface: Internet port
Keying: Aggressive mode (IKE)
Local address: Static IP address
Remote address: Dynamic IP address
Local Interface Gateway: DMZ port's gateway
Remote required endpoint ID: secondary@branch
Local network: 192.168.1.0/255.255.255.0
Remote network: 192.168.2.0/255.255.255.0

Branch Office SG configuration:

Tunnel name: SecondaryLink
Enable this tunnel: Unchecked
Local interface: Default gateway interface
Keying: Aggressive mode (IKE)
Local optional endpoint ID: secondary@branch
The remote party's IP address: 209.0.1.1
Local network: 192.168.2.0/255.255.255.0

Setup an unused aliased IP address on the LAN interface of both the Headquarter and Branch Office SnapGear appliances. For example:

Headquarters SG configuration:

Alias IP address: 192.168.11.1

Alias subnet mask: 24

Branch office SG configuration:

Alias IP address: 192.168.12.1

Alias subnet mask: 24

Set up a Primary Link Test IPSec tunnel between the primary Internet IP Addresses (192.168.11.0/32 - 209.0.0.1 <> 210.0.0.1 – 192.168.12.0/32). This will be used to determine whether the Primary Link is back up in the failed over state. Default values are used in the configuration unless otherwise specified below:

Headquarters SG configuration:

Tunnel name: PrimaryLinkTest

Local interface: Internet Port

Keying: Aggressive mode (IKE)

Local address: Static IP address

Remote address: Dynamic IP address

Local Interface Gateway: Internet port's gateway

Initiate phase 1 & 2 rekeying: Unchecked

Remote required endpoint ID: primarytest@branch

Phase 1 key lifetime (sec): 7200

Local network: 192.168.11.1/255.255.255.255

Remote network: 192.168.12.1/255.255.255.255

Phase 2 key lifetime (sec): 7200

Branch Office SG configuration:

Tunnel name: PrimaryLinkTest
Enable this tunnel: Unchecked
Local Interface: Default gateway interface
Keying: Aggressive mode (IKE)
Local optional endpoint ID: primarytest@branch
The remote party's IP address: 209.0.0.1
Local network: 192.168.12.1/255.255.255.255
Remote network: 192.168.11.1/255.255.255.255

Manually edit the `ifmond.conf` on both of the Branch Office SnapGear appliances to configure for IPSec failover and fall forward.



Important: *At least one space must precede any text for the indented subsections within the `ifmond.conf` file.*

```
##-- Custom entries MUST be added below this point
connection primarylinktest
    parent conn-eth1
    start ipsec auto --add PrimaryLinkTest
    start ipsec auto --up PrimaryLinkTest
    stop ipsec whack --delete --name PrimaryLinkTest
    maximum_retries 2147483647
    retry_delay 5
    test_delay 5
    test ifretry 2 5 ping -I 192.168.12.1 192.168.11.1 -c 3
connection primarylink
    parent primarylinktest
    start ipsec auto --add PrimaryLink
    start ipsec auto --up PrimaryLink
    stop ipsec whack --delete --name PrimaryLink
    maximum_retries 2147483647
    retry_delay 5
    test_delay 5
    test ifretry 2 5 ping -I 192.168.2.1 192.168.1.1 -c 3
```

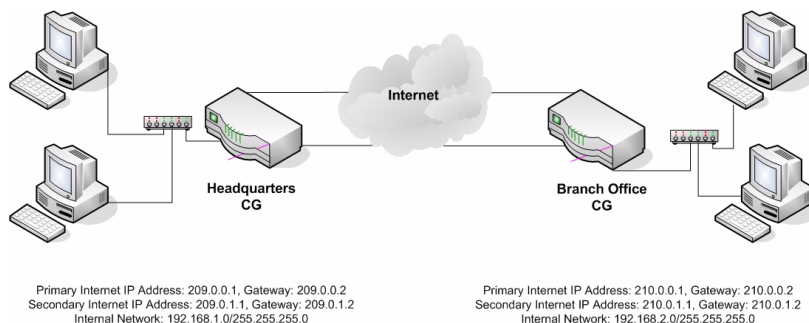
```

connection secondarylink
  parent conn-eth1
  start ipsec auto --add SecondaryLink
  start ipsec auto --up SecondaryLink
  stop ipsec whack --delete --name SecondaryLink
  maximum_retries 2147483647
  retry_delay 5
  test_delay 5
  test ifretry 2 5 ping -I 192.168.2.1 192.168.1.1 -c 3
service service-ipsec
  group primarylinktest
  group secondarylink

```

The following scenario assumes that the Headquarters SG and Branch Office SG each have two static Internet IP addresses. The Branch Office SG establishes an IPSec tunnel from its primary Internet IP address to the primary Internet IP address at the Headquarters SG as the primary IPSec tunnel path. If this IPSec connection is detected to have failed, a failover IPSec tunnel is established from the secondary Internet IP address to the secondary Internet IP address at the Headquarters SG. Once in the failover state, the Branch Office SG periodically determines if the primary IPSec tunnel path is functioning again, and if so, falls forward to use the primary link instead.

Figure 336: IPSec failover example two



Setup an IPSec tunnel between the primary Internet IP Addresses (209.0.0.1 <> 210.0.0.1). Default values are used in the configuration unless otherwise specified in the configuration that follows:

Headquarters SG configuration:

Tunnel name: PrimaryLink
Local interface: Internet port
Local Interface Gateway: Internet port's gateway
The remote party's IP address: 210.0.0.1
Local network: Address of Internet port
Remote network: Remote endpoint

Branch Office SG configuration:

Tunnel name: PrimaryLink
Local interface: Internet port
Local Interface Gateway: Internet port's gateway
The remote party's IP address: 209.0.0.1
Local network: Address of Internet port
Remote network: Remote endpoint

Setup an IPSec tunnel between the secondary Internet IP Addresses (209.0.1.1 <> 210.0.1.1). Default values are used in the configuration unless otherwise specified below:

Headquarters SG configuration:

Tunnel name: SecondaryLink
Enable this tunnel: Checked
Local interface: DMZ port
Local Interface Gateway: DMZ port's gateway
The remote party's IP address: 210.0.1.1
Local network: Address of DMZ port
Remote network: Remote endpoint

Branch Office SG configuration:

Tunnel name: SecondaryLink
Enable this tunnel: Checked
Local interface: DMZ port
Local Interface Gateway: DMZ port's gateway
The remote party's IP address: 209.0.1.1
Local network: Address of DMZ port
Remote network: Remote endpoint

Setup corresponding GRE tunnels over the IPSec tunnels configured in steps 1 and 2 (209.0.0.1 <> 210.0.0.1 and 209.0.1.1 <> 210.0.1.1). Default values are used in the configuration unless otherwise specified below:

Headquarters SG configuration:

GRE tunnel for primary link:

GRE tunnel name: PrimaryLink

Remote address: 210.0.0.1

Local address: 209.0.0.1

Firewall class: LAN

GRE tunnel for secondary link:

GRE tunnel name: SecondaryLink

Remote address: 210.0.1.1

Local address: 209.0.1.1

Firewall class: LAN

Branch Office SG configuration:

GRE tunnel for primary link:

GRE tunnel name: PrimaryLink

Remote address: 209.0.0.1

Local address: 210.0.0.1

Firewall class: LAN

GRE tunnel for secondary link:

GRE tunnel name: SecondaryLink

Remote address: 209.0.1.1

Local address: 210.0.1.1

Firewall class: LAN

Manually edit the `ifmond.conf` on both the Headquarter and Branch Office SG to configure for IPSec failover and fall forward.

Headquarters SG `ifmond.conf`:



Important: *At least one space must precede any text for the indented subsections within the `ifmond.conf` file.*

```
##-- Custom entries MUST be added below this point
connection primary_route
    parent primary_ping
    start route add -net 192.168.2.0 netmask 255.255.255.0
    dev gre1
    stop route del -net 192.168.2.0 netmask 255.255.255.0
    dev gre1
    maximum_retries 2147483647
    retry_delay 5
    test_delay 5
connection secondary_route
    parent secondary_ping
    start route add -net 192.168.2.0 netmask 255.255.255.0
    dev gre2
    stop route del -net 192.168.2.0 netmask 255.255.255.0
    dev gre2
    maximum_retries 2147483647
    retry_delay 5
    test_delay 5
connection primary_ping
    parent conn-gre1
    maximum_retries 2147483647
    retry_delay 5
    test_delay 5
    test ifretry 2 5 ping -I 209.0.0.1 210.0.0.1 -c 3
connection secondary_ping
    parent conn-gre2
    maximum_retries 2147483647
    retry_delay 5
    test_delay 5
    test ifretry 2 5 ping -I 209.0.1.1 210.0.1.1 -c 3
service service-ipsec
    group primary_ping
    group secondary_ping
```

Branch Office SG ifmond.conf:

**Important:** At least one space must precede any text for the indented subsections within the ifmond.conf file.

```

##-- Custom entries MUST be added below this point
connection primary_route
    parent primary_ping
    start route add -net 192.168.1.0 netmask 255.255.255.0
    dev gre1
    stop route del -net 192.168.1.0 netmask 255.255.255.0
    dev gre1
    maximum_retries 2147483647
    retry_delay 5
    test_delay 5
connection secondary_route
    parent secondary_ping
    start route add -net 192.168.1.0 netmask 255.255.255.0
    dev gre2
    stop route del -net 192.168.1.0 netmask 255.255.255.0
    dev gre2
    maximum_retries 2147483647
    retry_delay 5
    test_delay 5
connection primary_ping
    parent conn-gre1
    maximum_retries 2147483647
    retry_delay 5
    test_delay 5
    test ifretry 2 5 ping -I 210.0.0.1 209.0.0.1 -c 3
connection secondary_ping
    parent conn-gre2
    maximum_retries 2147483647
    retry_delay 5
    test_delay 5
    test ifretry 2 5 ping -I 210.0.1.1 209.0.1.1 -c 3
service service-ipsec
    group primary_ping
    group secondary_ping

```

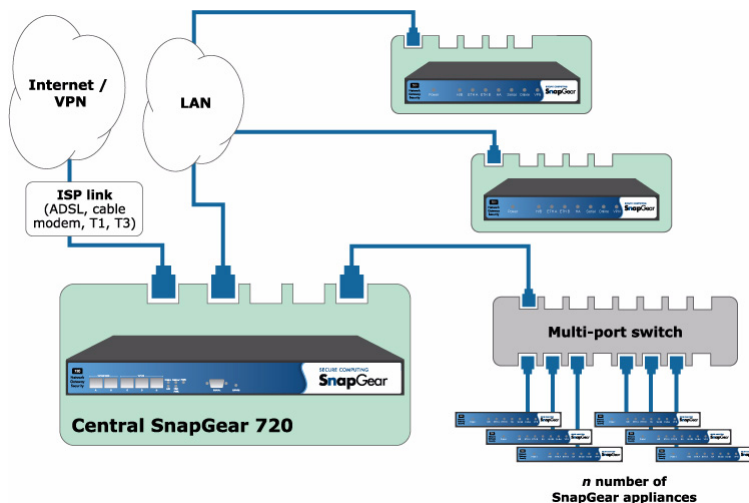
IPSec VPN offloading

IPSec VPN offloading improves overall tunnel counts and throughput by configuring additional SnapGear appliances as an offload device. An IPSec offload device is another Secure Computing SnapGear appliance that has been specifically configured to handle IPSec offloading. A single SG720 can manage about 400 IPSec tunnels. Using the offloading configuration, the number of IPSec tunnels can be doubled, tripled, or even quadrupled by adding more SnapGear appliances. This does not require any additional IP addresses. A single Internet IP address and one SnapGear management console can administer all of the tunnels. The offload device will handle the encryption and key processing required for all offloaded tunnels, thus greatly reducing the load on the main gateway device.

Note: Gateway and offload devices must be firmware 3.1.5 or later, and provide `sshd` services; therefore, the SG300 model cannot function as an offload device or primary gateway for VPN tunnel offloading purposes.

Figure 337 shows offloaded tunnels from the central SG720 appliance to SG580s through the LAN connection. It also illustrates using a multi-port switch to connect offload devices.

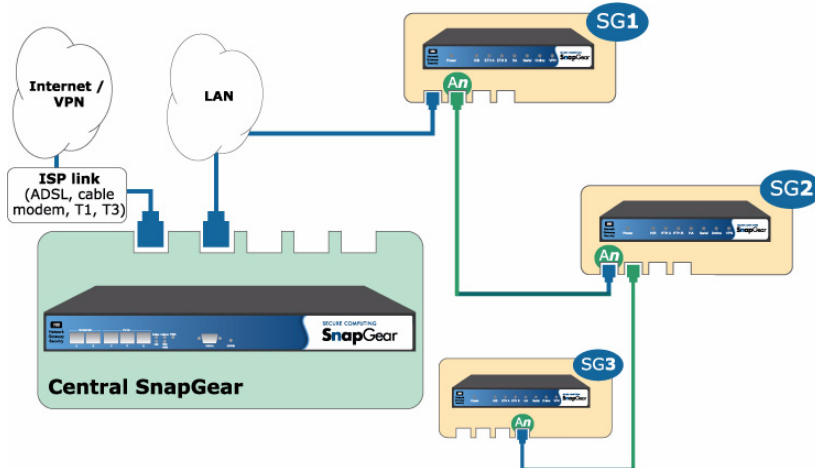
Figure 337: IPSec VPN offloading — Multi-port switch configuration



Offload devices can either be added to an existing switch on the LAN, or live on their own dedicated LAN segment and switch. If insufficient switch ports are available, it is possible to use the switch ports to chain offload devices together as they do not communicate with each other, and only require simple single-IP address visibility to the Central SnapGear appliance. The optimal arrangement for conserving switch ports is a tree layout. The switches should detect and resolve any wiring loops (802.1d) should any be inadvertently created. The four port switch is present on most SG appliances, except for the PCI SG 640 and SG720 rack mount appliances.

Figure 338 illustrates three daisy-chained SG580s (SG1, SG2, and SG3) that are connected via their **An** switch, which represents any port switch A1, A2, A3, or A4.

Figure 338: IPSec VPN offloading — Daisy-chain switch configuration



Offloading limitations

There are several limitations on the kinds of tunnels that can be offloaded:

- Only tunnels using IKE and PSK (preshared secrets) that operate on the default gateway can be offloaded.
- The remote endpoint of the tunnel must have a static IP address.
- The remote network or host must not be the remote endpoint IP address, or on the same network as the IP address of the remote endpoint.

For the most likely combinations, you will be prevented from selecting an incorrect combination.

To specify an offload device, you must initiate the Advanced wizard in IPSec. See “IPSec Advanced Setup wizard” on page 387. In addition to the wizard, there is some extra configuration required, as described in the next topic, “Configuring for VPN offloading” on page 446.

Configuring for VPN offloading

In addition to configuring the offload device within the advanced wizard, additional manual file configurations are required.



Important: Use the SnapGear management console to ensure changes are saved. For more information, see “Configuration Files tab” on page 519.

To set up IPSec offload devices, follow these instructions:

On the concentrator (primary or master) device:

Add the following line to the file `/etc/config/ssh_config`:

```
UserKnownHostsFile /etc/config/ssh_known_hosts
RhostsRSAAuthentication no RSAAuthentication no
```

Create the file `/etc/config/ssh_known_hosts` (or append the line to it if it already exists) containing the IP address of the IPSec offload device, followed by the contents of `/etc/config/ssh_host_rsa_key.pub` from the IPSec offload device.



Important: This new entry must all be on the same line without changes. Be sure to insert a space between the IP address and the key.

For example:

```
192.168.3.2 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAuUCgZGemo... =
```

On the IPSec offload device:

Add the following line to the file `/etc/config/sshd_config` using the management console to ensure changes are saved:

```
AuthorizedKeysFile /etc/config/authorized_keys
```

Create the file `/etc/config/authorized_keys` (or append to it if it already exists) and add into it the contents of `/etc/config/id_dsa.pub` from this offload device (the master, or concentrator).

Once the above configuration has been completed successfully, when logged in as root on this device, running the command `ssh hostname` should display the hostname of the IPSec offload device without requiring any passwords or prompts. Until this is configured and behaving as described, IPSec offload configuration will not allow offloading VPN tunnels.

Troubleshooting IPSec

IPSec tips

- Check the process table. When IPSec is enabled, it should show “pluto” is running. Pluto is the `isakmp` daemon listening on port 500. Check for a LISTEN on UDP port 500:

```
netstate -na | grep 500
```
- Use `tcpdump` to verify traffic. Internal traffic will be unencrypted. External traffic should show UDP 500 during tunnel establishment, and then ESP traffic for encrypted data; or UDP 4500 if NAT-T is negotiated successfully.
- Review the system log. There will be entries by Pluto with informative data.
- Verify the VPN LED is lit when the VPN tunnel is established (this LED applies to all types of VPN tunnels, not just IPSec).

IPSec symptoms, causes, and solutions

Symptom: IPSec is not running and is enabled.

Possible cause: The SnapGear appliance has not been assigned a default gateway.

Solution: Ensure the appliance has a default gateway by configuring the Internet connection on the Connect to Internet page or assigning a default gateway on the IP Configuration page.

Symptom: Tunnel is always down even though IPSec is running and the tunnel is enabled.

Possible causes:

- The tunnel is using Manual Keying and the encryption and/or authentication keys are incorrect.
- The tunnel is using Manual Keying and the appliance's and/or remote party's keys do not correspond to the Cipher and Hash specified.

Solution: Configure a correct set of encryption and/or authentication keys. Select the appropriate Cipher and Hash that the key have been generated from, or change the keys used to use the selected Cipher and Hash.

Symptom: Tunnel is always Negotiating Phase 1.

Possible causes:

- The remote party does not have an Internet IP address. A *No route to host* message is reported in the system log.
- The remote party has IPSec disabled (a *Connection refused* message is reported in the system log).
- The remote party does not have a tunnel configured correctly because:
 - The tunnel has not been configured.
 - The Phase 1 proposals do not match.
 - The secrets do not match.
 - The RSA key signatures have been incorrectly configured.
 - The Distinguished Name of the remote party has not be configured correctly.
 - The Endpoint IDs do not match.
 - The remote IP address or DNS hostname has been incorrectly entered.
 - The certificates do not authenticate correctly against the CA certificate.

Solution: Ensure that the tunnel settings for the appliance and the remote party are configured correctly. Also ensure that both have IPSec enabled and have Internet IP addresses. Check that the CA has signed the certificates.

Symptom: Tunnel is always Negotiating Phase 2.

Possible causes:

- The Phase 2 proposals set for the appliance and the remote party do not match.
- The local and remote subnets do not match.

Solution: Ensure that the tunnel settings for the appliance and the remote party are configured correctly. If phase 2 fails to come up when attempting a tunnel with a non-SnapGear appliance, such as a Sidewinder G2 or a TSP Classic appliance, selecting a Phase 2 Proposal with no Perfect Forward Secrecy is often the first step in ensuring compatibility between the endpoints.

Symptom: The tunnel appears to be up and I can ping across it, but HTTP, FTP, SSH, telnet, etc. do not work.

Possible cause: The MTU of the IPSec interface is too large.

Solution: Reduce the MTU of the IPSec interface.

Symptom: Tunnel goes down after awhile.

Possible causes:

- The remote party has gone down.
- The remote party has disabled IPSec.
- The remote party has disabled the tunnel.
- The tunnel on the appliance has been configured not to rekey the tunnel.
- The remote party is not rekeying correctly with the appliance.

Solution: Confirm that the remote party has IPSec and the tunnel enabled and has an Internet IP address. Ensure that the appliance has rekeying enabled. If the tunnel still goes down after a period of time, it may be due to the SnapGear appliance and remote party not recognizing the need to renegotiate the tunnel. This situation arises when the remote party is configured to accept incoming tunnel connections (as opposed to initiate tunnel connections) and reboots. The tunnel has no ability to let the other party know that a tunnel renegotiation is required. This is an inherent drawback to the IPSec protocol. Different vendors have implemented their own proprietary method to support the ability to detect whether to renegotiate the tunnel. Dead peer detection has been implemented based on the draft produced by Cisco Systems (*draft-ietf-IPSec-dpd-00.txt*). Unfortunately, unless the remote party implements this draft, the only method to renegotiate the tunnel is to reduce the key lifetimes for Phase 1 and Phase 2 for Automatic Keying (IKE). This does not occur for Manual Keying.

Symptom: Dead Peer Detection does not seem to be working.

Possible causes:

- The tunnel has Dead Peer Detection disabled.
- The remote party does not support Dead Peer Detection according to *draft-ietf-IPSec-dpd-00.txt*

Solution: Enable Dead Peer Detection support for the tunnel. Do not use Dead Peer Detection if the remote party does not support *draft-ietf-IPSec-dpd-00.txt*.

Symptom: Tunnels using x.509 certificate authentication do not work.

Possible causes:

- The date and time settings on the appliance has not been configured correctly.
- The certificates have expired.
- The Distinguished Name of the remote party has not been configured correctly on the appliance's tunnel.
- The certificates do not authenticate correctly against the CA certificate.
- The remote party's settings are incorrect.

Solution: Confirm that the certificates are valid. Confirm also that the remote party's tunnel settings are correct. Check the Distinguished Name entry in the appliance's tunnel configuration is correct.

Symptom: Remote hosts can be accessed using IP address but not by name

Possible cause: Windows network browsing broadcasts are not being transmitted through the tunnel.

Solutions:

- Set up a DNS/WINS server and use it to have the remote hosts resolve names to IP addresses.
- Set up HOSTS/LMHOST files on remote hosts to resolve names to IP addresses.

Symptom: Tunnel comes up but the application does not work across the tunnel.

Possible causes:

- There may be a firewall device blocking IPSec packets.
- The MTU of the IPSec interface may be too large.
- The application uses broadcasts packets to operate.

Solution: Confirm that the problem is the VPN tunnel and not the application being run. These are the steps you can try to find where the problem is (it is assumed that a network to network VPN is being used):

- 1** Ping from your PC to the Internet IP address of the remote party. This assumes that the remote party is configured to accept incoming pings.
If you cannot ping the Internet IP address of the remote party, either the remote party is not online or your computer does not have its default gateway as the SnapGear appliance.
- 2** Ping from your PC to the LAN IP address of the remote party.
If you can ping the Internet IP address of the remote party but not the LAN IP address, then the remote party's LAN IP address or its default gateway has not been configured properly. Also check your network configuration for any devices filtering IPSec packets (protocol 50) and whether your Internet Service Provider is filtering IPSec packets.
- 3** Ping from your PC to a PC on the LAN behind the remote party that the tunnel has been configured to combine.
If you can ping the LAN IP address of the remote party but not a host on the remote network, then either the local and/or remote subnets of the tunnel settings have been incorrectly configured or the remote host does not have its default gateway as the remote party.
If you can ping across the tunnel, then check if the MTU of the IPSec interface is allowing packets to go through. Reduce the MTU if large packets are not being sent through the tunnel.
If the application is still not working across the tunnel, then the problem is with the application. Check that the application uses IP and does not use broadcast packets since these are not sent across the IPSec tunnels. Contact the producer of the application for support.

Port tunnels

Port tunnels are point-to-point tunnels similar to regular VPNs, but only offer transport for a TCP service from one end of the tunnel to the other. This allows you to wrap a TCP service, such as Telnet or mail retrieval (POP3), in an HTTP or SSL connection. A single port tunnel can transport a single TCP port only.

The SnapGear appliance supports two kinds of port tunnels:

- HTTP tunnels (unencrypted)
- SSL tunnels (encrypted)

HTTP Tunnels are port tunnels that send data using the HTTP protocol and are not encrypted. HTTP tunnels can be useful when the appliance is behind a firewall that only allows outgoing HTTP connections and blocks all other traffic.

SSL Tunnels are port tunnels that send data using an encrypted SSL pipe. In order to use an SSL tunnel, you must first install an SSL certificate. For further information, see “Certificates for HTTPS” on page 210. SSL tunnels can be useful for encrypting TCP services that are by themselves unencrypted, such as a Telnet or FTP session.

The end of the port tunnel that is offering the TCP service (such as a Telnet or FTP server) must be configured as a Tunnel Server. The end of the port tunnel that is accessing the TCP service must be configured as a Tunnel Client.

You can create nested tunnels, such as a secure SSL tunnel over a HTTP tunnel. For more information, see “Creating nested port tunnels” on page 460.

The following procedures are provided in this topic:

- “Configuring an HTTP tunnel client” on page 453
- “Configuring an HTTP tunnel server” on page 455
- “Configuring an SSL tunnel client” on page 457
- “Configuring an SSL tunnel server” on page 458

Configuring an HTTP tunnel client

Use this procedure to configure an HTTP tunnel client that corresponds to an HTTP tunnel server.

- 1 From the **VPN** menu, click **Port Tunnels**. The Port Tunnels page appears.

Figure 339: Port Tunnels page

- 2 Select **HTTP Tunnel Client** from the tunnels list and click **Add**. The HTTP Tunnel Client page appears.

Figure 340: HTTP Tunnel Client page

- 3 Enter a descriptive name for the tunnel client in the **Name** field.
 - Can be one or more characters of any type
- 4 Ensure the **Enable** check box is selected. It is enabled by default.
- 5 In the **Data Port** field, enter the TCP port on which to listen for connections from local hosts to forward across the tunnel. This must match the TCP used by the application client.
 - Range: an integer value from 1-65535
- 6 Enter the publicly accessible IP address of the remote tunnel server in the **Tunnel Server** field.
- 7 Enter the TCP port on which the tunnel server is listening for connections in the **Tunnel Port** field. This must match the tunnel server's Tunnel Port.
 - Default: 80
 - Range: an integer value from 1-65535
- 8 [Optional] Specify the **Content Length** to use in HTTP PUT requests.
 - Default: 102400
 - Can be an integer value equal to or greater than 1
- 9 [Optional] To force Content Length for all requests, select the **Strict Content Length** check box. This setting always writes content-length bytes in requests.
- 10 To specify a maximum age for connections, after which the connection is closed, enter a value in seconds in the **Maximum Age** field.
 - Default: 300
 - Can be an integer value equal to or greater than 1
- 11 In the **Keep Alive** field, enter the interval at which to send keep alive bytes to keep the connection open.
 - Default: 5
 - Can be an integer value equal to or greater than 1

If you are not connecting to the HTTP tunnel server via an HTTP Proxy Server, disregard the remaining fields and skip to the last step, since your configuration for the client is complete. Otherwise, continue with the next step.
- 12 [Required for HTTP Proxy] If the client connects to the HTTP tunnel server via a proxy, enter the IP address in the **Proxy Server** field.
- 13 [Required for HTTP Proxy] Enter the TCP Port of the HTTP proxy in the **Proxy Port** field.
 - Default: 8080
 - Range: an integer value from 1-65535
 - Can be left blank
- 14 [Optional] If the proxy server requires authentication, enter the details in the **Proxy User name** and **Proxy Password** fields.
 - Can consist of any characters or be left blank

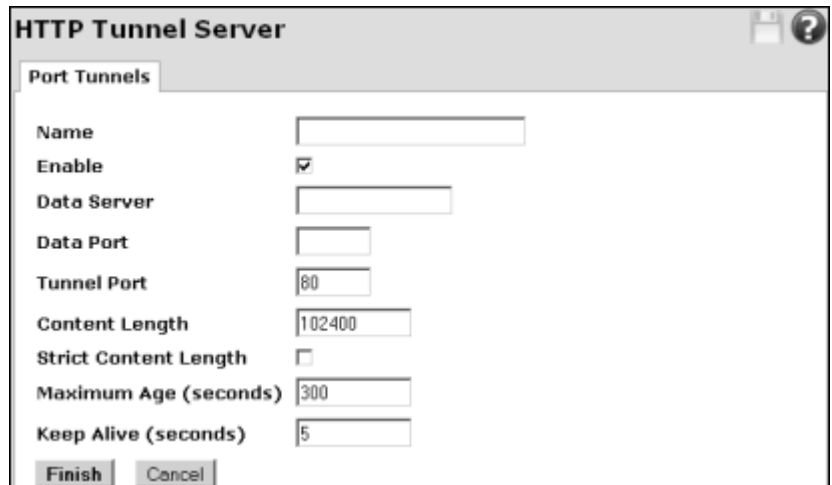
- 15 [Optional] If the proxy accepts connects from clients with a specific User Agent field only, enter it in **Proxy User Agent**.
 - Can consist of any characters or be left blank
- 16 Required for HTTP buffering proxy] If the HTTP proxy is a buffering proxy, enter the buffer size in the **Proxy Buffer Size** field. Otherwise, set this field to 0.
 - Default: 0
- 17 Specify the timeout before sending padding to fill up the buffer size in the **Proxy Padding Timeout** field.
 - Default: 500
- 18 Click **Finish**. Now configure the corresponding HTTP Server.

Configuring an HTTP tunnel server

Use this procedure to configure an HTTP tunnel server that corresponds to an HTTP tunnel client.

- 1 From the **VPN** menu, click **Port Tunnels**. The Port Tunnels page appears.
- 2 Select **HTTP Tunnel Server** from the tunnels list and click **Add**. The HTTP Tunnel Server page appears.

Figure 341: HTTP Tunnel Server page

The screenshot shows a window titled "HTTP Tunnel Server" with a "Port Tunnels" tab. The window contains several configuration fields: "Name" (empty text box), "Enable" (checked checkbox), "Data Server" (empty text box), "Data Port" (empty text box), "Tunnel Port" (text box with "80"), "Content Length" (text box with "102400"), "Strict Content Length" (unchecked checkbox), "Maximum Age (seconds)" (text box with "300"), and "Keep Alive (seconds)" (text box with "5"). At the bottom are "Finish" and "Cancel" buttons.

- 3 Enter a descriptive name for the tunnel server in the **Name** field. The name can be one or more characters of any type.
- 4 Ensure the **Enable** check box is selected. It is enabled by default.
- 5 Enter the IP address of the application server in the **Data Server** field.
- 6 Enter the TCP port of the application server in the **Data Port** field.
 - Range: an integer value from 1-65535

- 7 Enter the TCP port that the HTTP tunnel server accepts tunnel connections on in the **Tunnel Port** field. This must match the Tunnel Port used by the HTTP tunnel client.
 - Default: 80
 - Range: an integer value from 1-65535
- 8 [Optional] To specify the maximum length to use in HTTP PUT requests, enter a value in the **Content Length** field.
 - Default: 102400
 - Can be an integer value equal to or greater than 1
- 9 [Optional] To force the content length for all requests, select the **Strict Content Length** check box.
- 10 [Required if Strict Content Length is enabled] To specify a **Maximum Age** for connections after which the connection is closed, enter the number of seconds in the box.
 - Default: 300
 - Can be an integer value equal to or greater than 1
- 11 [Required if Strict Content Length is enabled] In the **Keep Alive** field, enter an interval in seconds at which to send keep alive bytes that keep the connection open.
 - Default: 5
 - Can be an integer value equal to or greater than 1
- 12 Click **Finish**.

Configuring an SSL tunnel client

Use this procedure to create an SSL tunnel client.

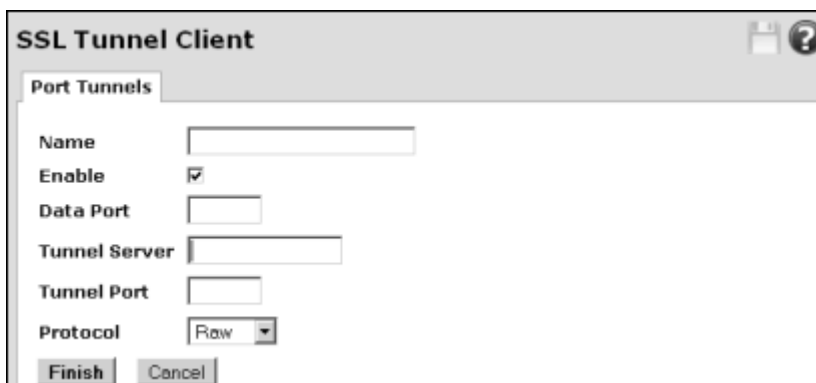
Prerequisites:

- Install an SSL certificate. For further information, see “Certificates for HTTPS” on page 210.

To create an SSL tunnel client

- 1 From the **VPN** menu, click **Port Tunnels**. The Port Tunnels page appears.
- 2 Select **SSL Tunnel Client** from the tunnels list and click **Add**. The SSL Tunnel Client page appears.

Figure 342: SSL Tunnel Client page

The image shows a window titled "SSL Tunnel Client" with a "Port Tunnels" tab. Inside the window, there are several configuration fields: "Name" (a text input field), "Enable" (a checked checkbox), "Data Port" (a text input field), "Tunnel Server" (a text input field), "Tunnel Port" (a text input field), and "Protocol" (a dropdown menu currently showing "Raw"). At the bottom of the window are two buttons: "Finish" and "Cancel".

- 3 Enter a descriptive name for the tunnel client in the **Name** field. The name can be one or more characters of any type.
- 4 Ensure the **Enable** check box is selected. It is enabled by default.
- 5 In the **Data Port** field, enter the TCP port on which to listen for connections from local hosts to forward across the tunnel. This must match the TCP port used by the application client.
 - Range: an integer value from 1-65535
- 6 Enter the publicly accessible IP address of the remote tunnel server in the **Tunnel Server** field.
- 7 Enter the TCP port on which the tunnel server is listening for connections in the **Tunnel Port** field.
 - Range: an integer value from 1-65535
- 8 Select the protocol to use when negotiating the SSL connection from the **Protocol** list. Available options are:
 - **Raw** [Default]
 - **CIFS**
 - **NNTP**

- **POP3**
- **SMTP**

To connect the tunnel client directly to an SSL server other than a tunnel server, select a Protocol value other than Raw. For example, select POP3 to configure a mail server to use POP3 over SSL.

9 Click **Finish**.

Configuring an SSL tunnel server

Use this procedure to create an SSL tunnel server.

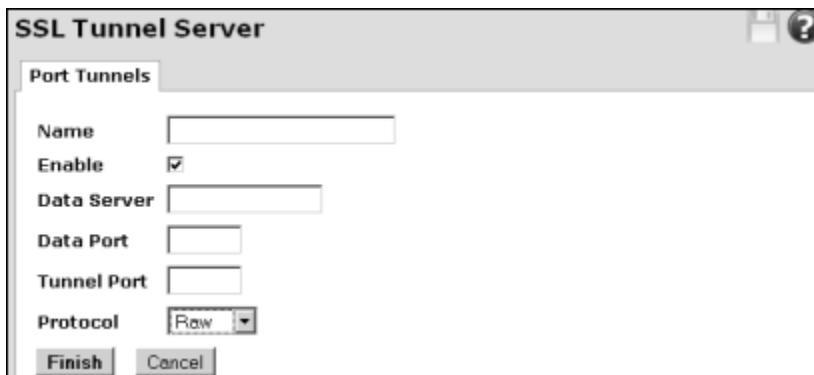
Prerequisites:

- Install an SSL certificate. For further information, see “Certificates for HTTPS” on page 210.

To create an SSL tunnel server

- 1 From the **VPN** menu, click **Port Tunnels**. The Port Tunnels page appears.
- 2 Select **SSL Tunnel Server** from the tunnels list and click **Add**. The SSL Tunnel Server page appears.

Figure 343: SSL Tunnel Server page

The image shows a window titled "SSL Tunnel Server" with a "Port Tunnels" tab. Inside the window, there are several fields: "Name" (a text box), "Enable" (a checked checkbox), "Data Server" (a text box), "Data Port" (a text box), "Tunnel Port" (a text box), and "Protocol" (a dropdown menu currently showing "Raw"). At the bottom of the window are "Finish" and "Cancel" buttons. A help icon (?) is visible in the top right corner of the window.

- 3 Enter a descriptive name for the tunnel server in the **Name** field. The name can be one or more characters of any type.
- 4 Ensure the **Enable** check box is selected. It is enabled by default.
- 5 Enter the IP address of the application server in the **Data Server** field.
- 6 Enter the TCP port of the application server in the **Data Port** field.
 - Range: an integer value from 1-65535
- 7 In the **Tunnel Port** field, enter the TCP port on which the SSL tunnel server accepts tunnel connections. This must match the Tunnel Port used by its corresponding SSL tunnel client.

- Range: an integer value from 1-65535
- 8 From the **Protocol** list, select the protocol to use when negotiating the SSL connection. Available options are:
 - **Raw** [Default]-Use the default when incoming connections are from a tunnel client.
 - **CIFS**
 - **NNTP**
 - **POP3**
 - **SMTP**

To connect the tunnel client directly to an SSL server other than a tunnel server, select a Protocol value other than Raw. For example, select POP3 to configure a mail server to use POP3 over SSL.

- 9 Click **Finish**.

Editing a port tunnel

- 1 From the **VPN** menu, click **Port Tunnels**. The Port Tunnels page appears.

Figure 344: Populated Port Tunnels page

Port Tunnels						
Port Tunnels						
	Name	Type	Data Endpoint	Tunnel Endpoint		
	1111	HTTP Tunnel Server	0.1.2.3:4	80		
	HTTP Tunnel Server	HTTP Tunnel Server	10.96.131.31:777	80		
	HTTP Tunnel client	HTTP Tunnel Client	777	10.96.131.31:80		
Add		HTTP Tunnel Client ▾				

- 2 Click the edit icon for the tunnel you want to edit. An edit page for the tunnel client or server appears.
- 3 Make your changes and click **Finish**.

Disabling a port tunnel

- 1 From the **VPN** menu, click **Port Tunnels**. The Port Tunnels page appears.
- 2 Click the edit icon for the tunnel you want to edit. An edit page for the tunnel client or server appears.
- 3 Clear the **Enable** check box and click **Finish**.

Deleting a port tunnel

- 1 From the **VPN** menu, click **Port Tunnels**. The Port Tunnels page appears.
- 2 Click the delete icon for the tunnel you want to delete. A message prompts you to confirm the delete. Click OK.

Creating nested port tunnels

It is possible to create nested tunnels, which is useful for creating a secure SSL tunnel over an HTTP tunnel.

- 1 Create the HTTP tunnel client and server.
- 2 Create a SSL tunnel client such that the Tunnel Endpoint of the SSL tunnel client matches the Data Endpoint of the HTTP tunnel client. Specify `127.0.0.1` for the Tunnel Server field of the SSL tunnel client.
- 3 Create a SSL tunnel server such that the Tunnel Endpoint of the SSL tunnel server matches the Data Endpoint of the HTTP tunnel server. Specify `127.0.0.1` for the Data Server field of the HTTP tunnel server.

CHAPTER 5

System menu features

In this chapter...

Date and Time menu	462
Backup/Restore menu	469
Users menu	476
Management menu	486
Diagnostics menu	497
Advanced menu	511

Date and Time menu

Use this menu to set the date and time on the SnapGear appliance. Setting the appliance clock to the correct date and time is important; otherwise, the timestamps of system log messages do not match the time of the event. If you use certificates for SSL or IPSec, it is especially important that you set the date and time correctly, as certificates include a start date and time before which they do not function and an expiry date and time after which they do not function. All changes to the time are logged in the System Log to assist with tracking a chain of events.



Important: *If an appliance is located such that it is subject to the extended Daylight Savings Time trial, firmware version 3.1.4u5 and higher automatically accommodate the adjustment. The Extended DST trial only applies to Canada, the United States of America, and Western Australia. If you are running firmware prior to 3.1.4u5, you must manually adjust your time settings. For more information, refer to article #3146 in the SnapGear Knowledgebase <http://sgkb.securecomputing.com>.*

When the time and date is set through the management console, or retrieved from an NTP server, the hardware clock of the SnapGear appliance is automatically updated. The hardware clock uses a battery to allow the current time and date to be maintained across reboots, and after the appliance has been powered down for longer periods of time.

Setting locality

Setting a locale (time zone) is only relevant if you are synchronizing with an NTP server or your SnapGear appliance has a real time clock (all but the SG300 have a real time clock). After you select your local region, the system clock shows local time. Without setting locale, the system clock shows UTC (Coordinated Universal Time) time.

Prerequisite: You must set your Locality before you set the date and time.

- 1 From the **System** menu, click **Date and Time > Locality** tab. The Locality page appears.

Figure 345: Locality tab

Date and Time Configuration

Set Date and Time | NTP Time Server | **Locality**

Locality

The locality setting allows your SnapGear unit to be configured for operation in a specific area. The primary effect of this setting is to allow times and dates to be displayed using local time (in conjunction with an operating NTP server).

Before setting the date and time on the SnapGear unit, you must set the Locality. Once this is done, you may set the date and time either **manually** or via the **NTP Time Server** page.

Region: US/Central

Submit

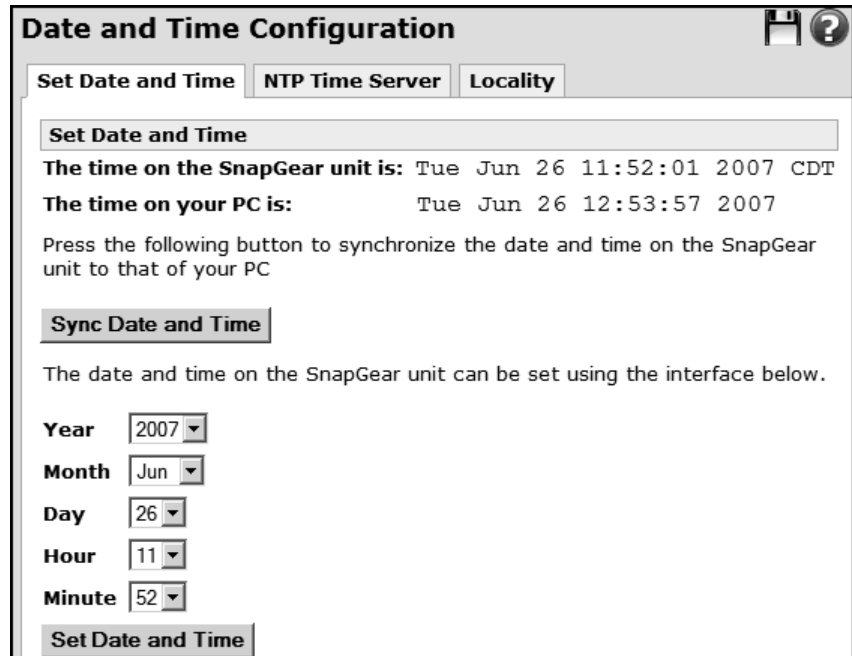
- 2 Select your local region from the **Region** list.
- 3 Click **Submit**.

Syncing appliance date and time with a PC

Use this procedure to set the date and time of your appliance to a personal computer. You must have JavaScript enabled in your Web browser to sync your appliance time with your PC.

- 1 From the **System** menu, click **Date and Time**. The Set Date and Time page appears.

Figure 346: Set Date and Time tab



The screenshot shows a web interface titled "Date and Time Configuration" with a save icon and a help icon in the top right. Below the title is a tabbed interface with three tabs: "Set Date and Time" (selected), "NTP Time Server", and "Locality". Under the "Set Date and Time" tab, there is a sub-header "Set Date and Time". The main content area displays two time comparisons: "The time on the SnapGear unit is: Tue Jun 26 11:52:01 2007 CDT" and "The time on your PC is: Tue Jun 26 12:53:57 2007". Below this, a text prompt says "Press the following button to synchronize the date and time on the SnapGear unit to that of your PC". A large button labeled "Sync Date and Time" is centered. Below the button, a text line states "The date and time on the SnapGear unit can be set using the interface below." This is followed by a series of dropdown menus for "Year" (2007), "Month" (Jun), "Day" (26), "Hour" (11), and "Minute" (52). At the bottom of this section is a button labeled "Set Date and Time".

- 2 Click **Sync Date and Time**. You can compare the current times between the SnapGear appliance and your PC.

Manually setting the appliance date and time

Use this procedure to manually set the date and time of your appliance. If your appliance does not have a hardware clock, the recommended method for setting the date and time is using network time. See “Enabling the NTP time server” on page 465. In rare circumstances, it may be desirable for the time on the appliance not to be synchronized to a PC or NTP server, which is when you can use the manual configuration method to artificially set the appliance to any time between 2002 and 2030.

- 1 From the **System** menu, click **Date and Time**. The Set Date and Time page appears.
- 2 Select the **Year**, **Month**, **Date**, **Hour**, and **Minute** from the lists.
- 3 Click the lower **Set Date and Time**. An action successful message is displayed and the time is set to your selections.

Enabling the NTP time server

Use this procedure to configure the Network Time Protocol (NTP) services on the SnapGear appliance. The appliance can make use of an NTP server or peer running the NTP to provide for time synchronization across a network. The appliance uses NTP version 4.0.

Be sure to set the Locality correctly before enabling the NTP features of the SnapGear appliance. See “Setting locality” on page 463 for instructions.

- 1 From the **System** main menu, click **Date and Time > NTP Time Server** tab. The NTP Time Server page appears.

Figure 347: NTP Time
Server tab

The screenshot shows a web-based configuration interface titled "Date and Time Configuration". It has three tabs: "Set Date and Time", "NTP Time Server" (which is selected), and "Locality".

Under the "NTP Time Server" tab, there is a section titled "NTP Time Server" with the following text: "The network time (NTP) server sets the system time so that it is synchronized with a remote time server. This ensures that the SnapGear unit's clock will be kept extremely accurate. The NTP server also acts as a local time server for hosts on the local network to synchronize their clocks with the SnapGear unit's (synchronized) clock. A Remote Peer can also synchronize its clock to this unit, as well as this unit synchronizing to it."

Below the text, there is an "Enabled" checkbox, which is currently unchecked. To the right of the checkbox is a "Submit" button.

Below the "Submit" button is a section titled "NTP Hosts". It contains a table with two columns: "Host" and "Type". The table is currently empty, with the text "No entries" displayed below the column headers.

Below the table, there is an "IP Address" input field, a "Type" dropdown menu (currently set to "Server"), and an "Add" button.

- 2 In the **NTP Time Server** pane, select the **Enabled** check box.
- 3 Click **Submit**. You can now add an NTP server or peer. See "Adding an NTP server" on page 468 and "Adding an NTP peer" on page 468.

Synchronizing clocks to the SnapGear appliance

Local hosts can synchronize their clocks to the SnapGear appliance by specifying the IP address of their appliance as their network time server in the Windows Date and Time Properties dialog box.

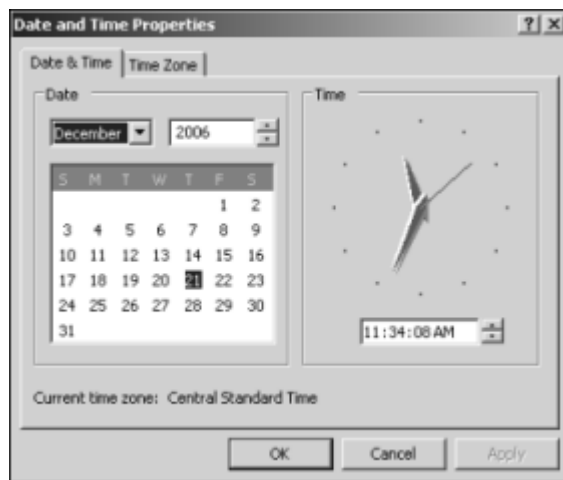
Prerequisite: The host running Windows must not be connected to a domain controller.

To synchronize a clock to SnapGear:

- 1 In Windows XP, click **Start > Settings > Control Panel > Date and Time > Internet Time** tab.
- 2 Enter the IP address of the SnapGear appliance as the Network Time Server.
- 3 Click **OK**.

In computers running Windows XP, the Date and Time Properties dialog box provides an Internet Time tab wherein you can configure which NTP server Windows should use. This tab is not available if Windows is connected to a domain controller, as Microsoft automatically configures the domain controller as the Network Time Server. Figure 348 shows the Date and Time Properties dialog box for a Windows XP computer connected to a domain controller, thus no Internet Time tab is available.

Figure 348: Windows XP
Date and Time dialog box



Adding an NTP server

The SnapGear appliance can synchronize its system time with a remote time server using the network time protocol (NTP). Adding an NTP server ensures the clock in the SnapGear appliance is accurate soon after the Internet connection is established.

More than one NTP server can be added. The appliance considers the response from each server and uses provisions in the network time protocol to determine the most accurate date and time.

When synchronizing with an NTP server, the date and time is displayed in UTC. To display local time, you must set the Locality appropriately. For more information, see “Setting locality” on page 463.

- 1 From the **System** menu, click **Date and Time > NTP Time Server** tab. The NTP Time Server page appears.
- 2 In the **NTP Time Server** pane, enter the address of the remote time host in the **IP Address** field.
- 3 Select **Server** from the **Type** list.
- 4 Click **Add**. The NTP server is displayed in the Host and Type list. You can delete the server by clicking the delete icon next to the server name.

Figure 349: NTP Host

Host	Type
100.1.1.99	Server

IP Address

Type

Adding an NTP peer

While NTP servers only offer the time to NTP clients, NTP peers both offer and accept time updates from each other. A possible suitable NTP peer for the SnapGear appliance is another NTP server on your local network.

- 1 From the **System** menu, click **Date and Time > NTP Time Server** tab. The NTP Time Server page appears.
- 2 In the **NTP Time Server** pane, enter the **IP Address** of the NTP server.
- 3 Select **Peer** from the **Type** list.
- 4 Click **Add**. The NTP Peer is displayed in the Host list.

Backup/Restore menu

In the unlikely event that your SnapGear appliance should lose its configuration or require a factory erase, you can restore a configuration stored on a PC, USB storage device, or some other safe place to minimize downtime.



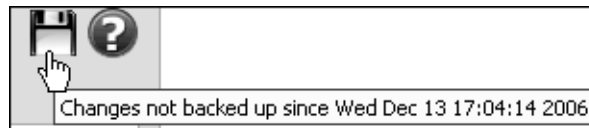
Caution: Firmware versions and model numbers are not checked when restoring a configuration. Therefore, ensure you restore a configuration only to the same SnapGear appliance model and firmware version from which you backed up the configuration.

A copy of your current configuration can also be stored on the SnapGear appliance itself. This is useful for storing multiple configuration profiles, or as a quick snapshot of a known good configuration before any configuration changes are made that cause the appliance to stop functioning as before. Configuration can also be saved as a plain, unencrypted text file.

After configuring your SnapGear appliance, it is strongly recommended that you remotely back up your configuration to an encrypted file. If the appliance becomes unresponsive and you cannot contact the appliance, a factory erase might be necessary. A factory erase eradicates locally stored configurations. Therefore, the locally stored configuration files should not be considered a substitute for performing regular, remote configuration backups. A best practice is to backup a configuration remotely on a regular basis before and after any configuration changes.

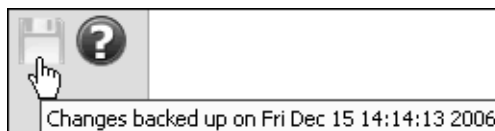
The backup/restore icon is available on every page in the Web management console. To display the date on which configuration changes were last backed up, hover your mouse pointer over the backup/restore icon. If the icon is black, and the text “Changes not backed up since *date*” is displayed, the configuration backup is not current and should be done as soon as possible. The date of the last backup is displayed. Click the icon to quickly access the Remote Configuration Backup/Restore page.

Figure 350: Viewing Backup Configuration Dates



Click the icon to backup the current configuration or restore a backed up configuration.

Figure 351: Viewing Backup Configuration Dates



If the icon is grayed and unavailable, the backup is current.

Remote Backup/Restore page

Use this page to backup and restore configuration files saved to a personal computer.

Backing up a configuration remotely

A remote backup saves the configuration file to a password-encrypted file on a personal computer.

- 1 From the **System** menu, click **Backup/Restore**. The Remote Configuration Backup/Restore page appears.

Figure 352: Remote Configuration Backup/Restore

Remote Configuration Backup/Restore

Remote Backup/Restore Local Backup/Restore Text Save/Restore

The SnapGear unit provides a method to backup and restore the entire configuration in a secure manner to your computer's hard drive or another remote location. All the unit's configuration will be saved to or restored from a single file that contains cryptographic protection and integrity checking.

Save Configuration

Backup the entire configuration of this SnapGear unit as a file on your computer.

Password

Confirm Password

Unencrypted ☐

Save

Restore Configuration

Select the file which you'd like to restore from.

Restore from file **Browse...**

Password

Restore

- 2 [Conditional; complete if not saving an unencrypted configuration.] Enter a password in the **Password** field with which to protect this file.
- 3 [Conditional; complete if not saving an unencrypted configuration.] Enter the password again in the **Confirm Password** field.



Caution: Ensure this is a hard-to-guess password, as all passwords including IPsec passwords and private keys are downloaded into your saved configuration. Ensure your password is easy to remember. If this password is lost, there is no way to restore your configuration.

- 4 [Optional] To save an unencrypted configuration backup, select the **Unencrypted** check box. You must leave the password fields blank if you enable this option.



Security Alert: *Ensure the configuration is transferred over an encrypted connection and stored on a secured system. This file is not intended to be human-readable, although some portions can be read. The format is similar to files created with the Text Save/Restore option.*

- 5 Click **Submit**. You are prompted to save the file. Click **Save** and save the file in a safe place.

Restoring a remote configuration

Use this procedure to restore a configuration you saved remotely from the appliance to your personal computer.

- 1 From the **System** menu, click **Backup/Restore**. The Remote Backup/Restore tab appears.
- 2 Click **Browse** to locate the .sgc configuration file you previously backed up.
- 3 Enter the password for the configuration file in the **Password** field.
- 4 Click **Submit**.

Local Backup/Restore page

Use the Local Backup/Restore page to backup and restore configuration files locally, which means on the SnapGear appliance itself.



Caution: If a factory erase is performed, backup files are erased. Using Remote Backup/Restore is highly recommended. See “Backing up a configuration remotely” on page 470.

Saving a configuration locally

Each local configuration backup stores a single snapshot of the configuration only; existing configuration snapshots on the SnapGear appliance are not saved embedded inside any subsequent snapshots.

- 1 From the **System** menu, click **Backup/Restore > Local Backup/Restore** tab. The Save Configuration page appears.

Figure 353: Local Configuration Backup/Restore

Local Configuration Backup/Restore

Remote Backup/Restore Local Backup/Restore Text Save/Restore

Save Configuration

Store a snapshot of the current configuration on the SnapGear unit itself.

Description SecureComputing-SG565

Save

Restore or Delete Configuration

Select a configuration to restore or delete.

Date	Time	Description
No entries		





- 2 [Optional] Enter a **Description** for this configuration. It is not necessary to include the time and date in the description since they are recorded automatically.
- 3 Click **Save**.

Restoring a local configuration

Use this procedure to restore a locally backed up configuration file. Restoring a remote or local configuration snapshot does not remove existing local configuration snapshots; a copy of the configuration remains.

- 1 From the **System** menu, click **Backup/Restore > Local Backup/Restore** tab. The Save Configuration page appears.
- 2 Restore a locally backed up configuration by click its corresponding **Restore** icon in the **Restore or Delete Configuration** pane.

Figure 354: Restore or Delete Local Configuration

Restore or Delete Configuration				
Select a configuration to restore or delete.				
Date	Time	Description		
20061213	16:45:09	SecureComputing-SG565		
20061213	16:45:03	SecureComputing-SG565		

- 3 A message requests you to confirm the restore. Click **OK**. A message indicates the appliance is restored and rebooting.

Deleting a local configuration file

Use this procedure to delete a saved local configuration file no longer needed.

- 1 From the **System** menu, click **Backup/Restore > Local Backup/Restore** tab. The Save Configuration page appears.
- 2 Delete a locally backed up configuration by click its corresponding **Delete** icon in the **Restore or Delete Configuration** pane.
- 3 A message requests you to confirm the delete. Click **OK**. The local configuration file is deleted and no longer appears in the configuration list.

Text save/restore tab

Use this page to save and restore a configuration to and from a text file.

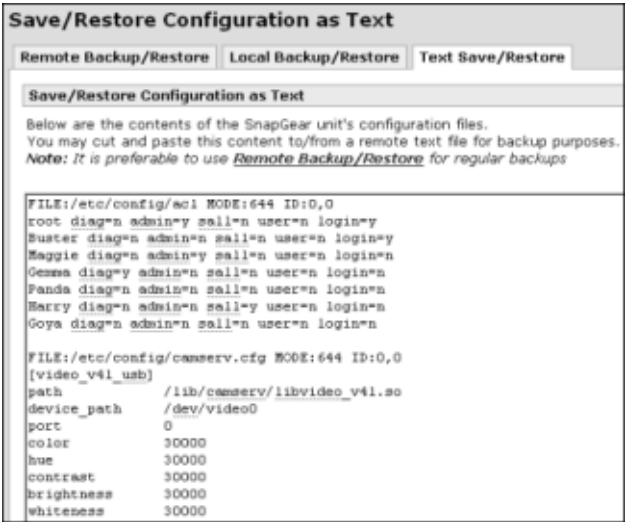


Caution: Some passwords and keys used in the appliance, such as for PPTP and IPSec, are stored unencrypted. Since plain text files are prone to undetected corruption, ensure the plain text backup is stored in a secure manner. Secure Computing recommends using **Remote backup/restore** for regular backups instead of text file backups. See “Backing up a configuration remotely” on page 470.

Saving a configuration to a text file

- 1 From the **System** menu, click **Backup/Restore > Text Save/Restore** tab. The Save/Restore Configuration as Text page appears.

Figure 355: Text Save/
Restore tab



- 2 Copy and paste the configuration files from the text box to a plain text file stored on a PC.

Restoring a saved configuration text file

- 1 From the **System** menu, click **Backup/Restore > Text Save/Restore** tab. The Save/Restore Configuration as Text page appears.
- 2 Cut and paste the text from the saved file to the configuration file text box.



Caution: Exercise care when copying and pasting configurations in this page. If the information pasted is incorrect or corrupted, you may have to perform a recovery procedure, which is provided in Appendix B.

- 3 Scroll to the bottom of the file and click **Submit**.

- 4 Reboot to apply the changes.

Users menu

This section details adding administrative as well as local users for PPTP, L2TP, or dial-in access, or access through the access control Web proxy.

Administrative users page

Administrative user accounts on a SnapGear appliance allow administrative duties to be spread amongst a number of different people according to their level of competence and trust. Each administrative user has a password they use to authenticate when connecting to the Web management console, or via telnet or ssh. They also have a number of access controls that modify what they can and cannot do via the Web management console.

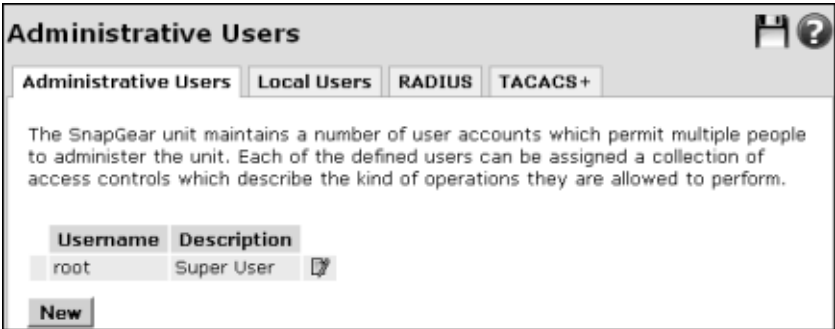
There is one special user, *root*, who has the role of the final administrative user, or super user. The access privileges for the root user cannot be lowered, and the root user cannot not be deleted or disabled. You can disallow telnet or ssh connections using the root account, however.

Administrative users are distinct from Local users in that the Administrative users cannot be given rights to connect via VPN or authenticate using the Internet access controls.

Creating an administrative user

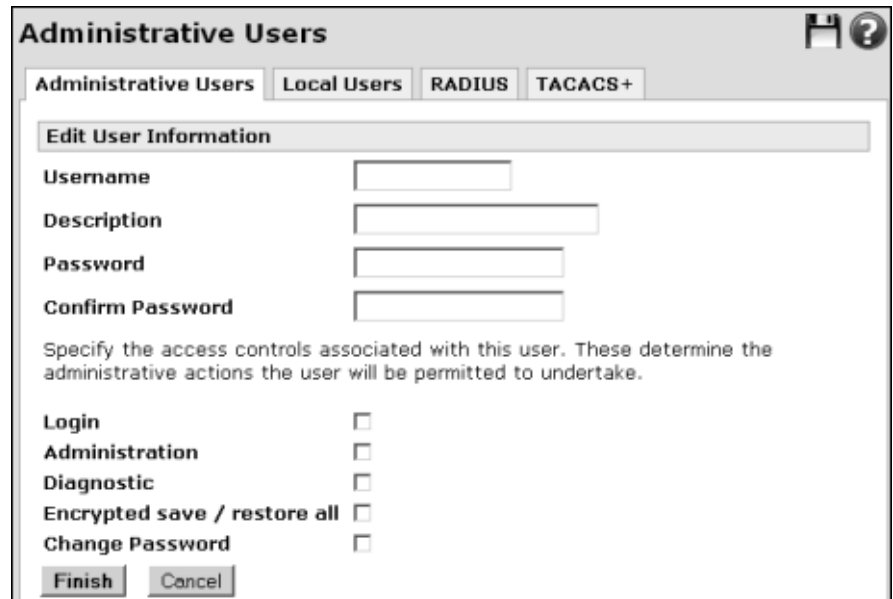
- 1 From the **System** menu, click **Users**. The Administrative Users page appears.

Figure 356:
Administrative Users —
New



- 2 Click **New**. The Edit User Information page appears.

Figure 357:
Administrative Users —
Edit User Information



The screenshot shows a web interface titled "Administrative Users" with a help icon in the top right. Below the title are four tabs: "Administrative Users" (selected), "Local Users", "RADIUS", and "TACACS+". The main section is titled "Edit User Information" and contains the following fields and options:

- Username**: A text input field.
- Description**: A text input field.
- Password**: A text input field.
- Confirm Password**: A text input field.

Below these fields is a paragraph: "Specify the access controls associated with this user. These determine the administrative actions the user will be permitted to undertake."

Then, there are five checkboxes, each with a label to its left:

- Login** ☐
- Administration** ☐
- Diagnostic** ☐
- Encrypted save / restore all** ☐
- Change Password** ☐

At the bottom are two buttons: "Finish" and "Cancel".

- 3 Enter a **Username** (login name). The username must start with an alphabetic character, but can consist of alphanumeric characters.
- 4 [Optional] Enter a description of the user in the **Description** field.
- 5 Enter a password in the **Password** field. The password can be one or more characters of any type.
- 6 Confirm the password in the **Confirm Password** field.
- 7 You can specify the following access controls for each administrative user:
 - To provide the user with telnet and ssh access to the command-line administration interface of the SnapGear appliance, select the **Login** check box.
 - To give the user the ability to make changes to the SnapGear appliance's configuration via the Web-based administration interface, select the **Administration** check box. This should only be provided to trusted users who are permitted to configure and reconfigure the appliance.
 - To provide the user with the ability to view restricted diagnostic information via the Web-based administration interface, select the **Diagnostic** check box. This access control can be given to technical support users so they can attempt to diagnose but not fix any problems that occur.

- To provide the user with the ability to save and restore the configuration of the SnapGear appliance via the Save/Restore page, select the **Encrypted save / restore all** check box. This access control can be given to a technician to whom you want the ability to restore the appliance to a known good configuration but to whom you do not want to grant full administration rights.



Caution: A user with **Encrypted save / restore all** access can conceivably create an encrypted config file with an arbitrary root password that they can restore, thus granting them Administration privileges. Therefore, grant **Encrypted save / restore all** only to users that you trust with **Administration** access.

- To provide the user with the ability to change their password via the Web management console, select the **Change Password** check box.

8 Click **Finish**. The administrative user is displayed in the edit box and is enabled by default.

To disable an administrative user, clear the check box next to their name. The user Buster is disabled in Figure 358:

Figure 358:
Enabled and Disabled
Admin Users

	Username	Description		
	root	Super User		
<input type="checkbox"/>	Buster	Telecommuter		
<input checked="" type="checkbox"/>	Gemma	Troubleshooter		
<input checked="" type="checkbox"/>	Maggie	Admin		
New				

Editing an administrative user

- 1 From the **System** menu, click **Users**. The Administrative Users page appears.
- 2 Click the edit icon next to their username. The Edit User Information page is displayed.
- 3 Make your changes and click **Finish**.

Deleting an administrative user

Note: The root user cannot be deleted.

- 1 From the **System** menu, click **Users**. The Administrative Users page appears.
- 2 Click the delete icon next to their username.
- 3 Confirm the delete. The user is removed from the list of users.

PCI DSS page

Use this page to configure partial compliance with the PCI DSS (Payment Card Industry Data Security Standard) user authentication and password management standard. A future firmware revision will feature full compliance.

- 1 From the **System** menu, click **Users**. The Administrative Users page appears.
- 2 Click the **PCI DSS** tab. The Payment Card Industry Data Security Standard page appears.

Figure 359:
Administrative Users —
PCI DSS page

Payment Card Industry Data Security Standard

Administrative Users Local Users RADIUS TACACS+

Administrative Users PCI DSS

Enabled ☐

Failed attempts before locking unit

Lock out time period

Number of database records to maintain

Submit

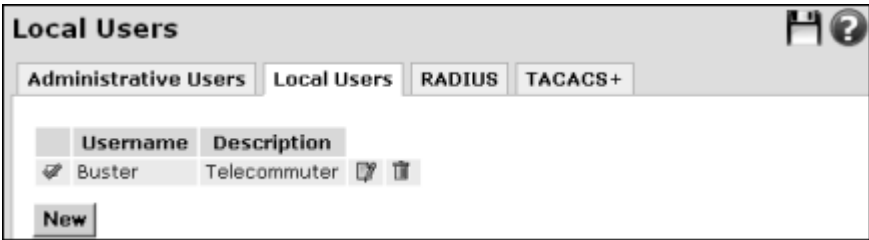
- 3 To lock out users from the appliance after failed administrative authentication attempts, select the **Enabled** check box.
- 4 Enter a the number of failures to permit before locking the appliance in the **Failed attempts before locking unit** field.
 - Default: 5
 - Can be an integer equal to or greater than 1
- 5 Enter a value for the duration of the lock out in seconds in the **Lock out time period** field.
 - Default: 1800 s (30 minutes)
 - Can be 0 or greater
- 6 Specify the size of the administrative user authentication failure database in the **Number of database records to maintain** field. It is safe to set this value larger than the number of administrative users to ensure all failed administrator logins are recorded in the database.
 - Default: 100
 - Can be an integer equal to or greater than 1
- 7 Click **Submit**.

Adding a local user

Use this procedure to add a local user. Local users accounts are used to grant PPTP, L2TP, or dial-in access, and access through the access control Web proxy.

- 1 Click **System > Users > Local Users** tab. The Local Users page is displayed.

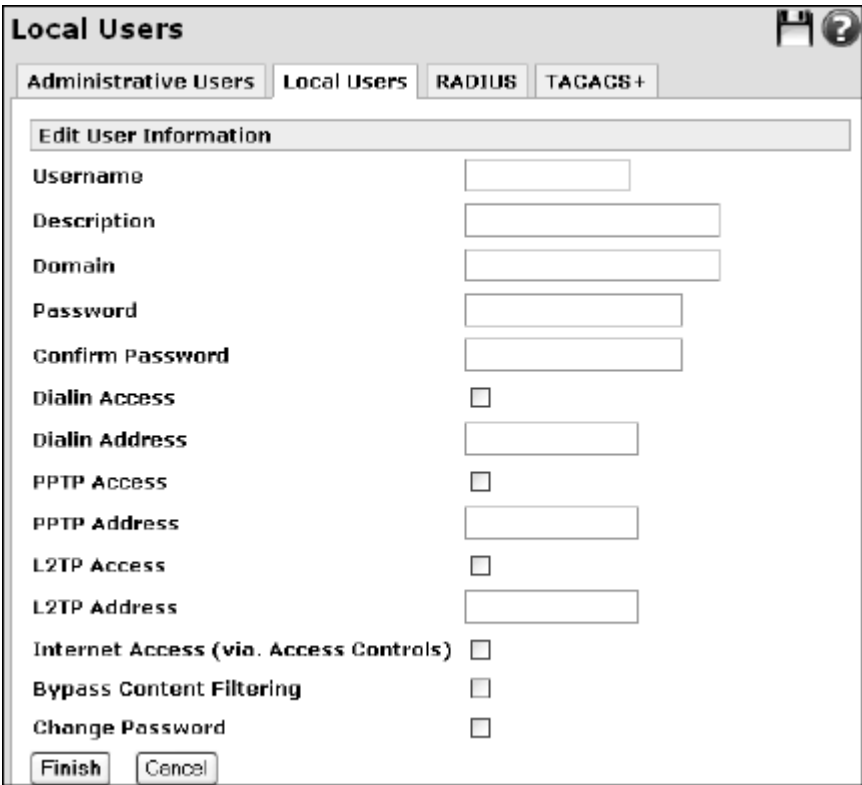
Figure 360:
Local Users page



The screenshot shows the 'Local Users' page. At the top, there are four tabs: 'Administrative Users', 'Local Users' (which is selected), 'RADIUS', and 'TACACS+'. Below the tabs is a table with two columns: 'Username' and 'Description'. The table contains one entry: 'Buster' with the description 'Telecommuter'. To the right of the 'Buster' entry are two icons: a document with a pencil and a trash can. Below the table is a 'New' button. In the top right corner of the page, there are icons for a floppy disk and a question mark.

- 2 Click **New**. The Edit User Information page appears.

Figure 361:
Local Users Edit User
Information page



The screenshot shows the 'Local Users Edit User Information' page. At the top, there are four tabs: 'Administrative Users', 'Local Users' (which is selected), 'RADIUS', and 'TACACS+'. Below the tabs is a form titled 'Edit User Information'. The form contains the following fields and options: 'Username' (text input), 'Description' (text input), 'Domain' (text input), 'Password' (text input), 'Confirm Password' (text input), 'Dialin Access' (checkbox), 'Dialin Address' (text input), 'PPTP Access' (checkbox), 'PPTP Address' (text input), 'L2TP Access' (checkbox), 'L2TP Address' (text input), 'Internet Access (via. Access Controls)' (checkbox), 'Bypass Content Filtering' (checkbox), and 'Change Password' (checkbox). At the bottom of the form are two buttons: 'Finish' and 'Cancel'. In the top right corner of the page, there are icons for a floppy disk and a question mark.

- 3 Enter a login name in the **Username** field. The name must start with an alphabetic character but can consist of alphanumeric characters and underscores.
- 4 [Optional] Enter a **Description**.
- 5 For Dial-in, PPTP, and L2TP Access users, you can enter a **Domain** name if your network has a Windows domain server.
 - Must be uppercase. If not entered in uppercase, this field entry is automatically converted to uppercase for Windows compatibility.
- 6 Enter a password for the user in the **Password** field. This is the password the user enters when accessing the local services of the SnapGear appliance. If you are editing a local user, you can leave the password field blank and the original password is still retained.
 - Minimum characters: 1
 - Can consist of any characters



Important: *If you have an older version of the Windows operating system, limit the password to 14 maximum characters.*

- 7 [Conditional, if Password field completed] Enter the password again in the **Confirm Password** field.
- 8 Specify the following access controls for each local user:
 - To provide the user with the authority to connect to the dial-in server of the appliance, select the **Dial-in Access** check box.
 - [Optional] To assign a fixed IP address when the user connects to the dialin server of the appliance, enter the IP address in the **Dialin Address** field.
 - To provide the user with the authority to connect to the PPTP VPN server of the appliance, select the **PPTP Access** check box.
 - [Optional] To assign a fixed IP address when the user connects to the PPTP VPN server of the appliance, enter the IP address in the **PPTP Address** field.



Important: *Users with a fixed IP address still require a dynamic IP address even though they do not use it. The PPTP VPN Server dynamic IP address range must be large enough to accommodate users with both dynamic and fixed addresses. If IP addresses are in short supply, the unused dynamic IP addresses can be used for other purposes.*

- To provide the user with the authority to connect to the L2TP server of the appliance, select the **L2TP Access** check box.

- [Optional] To assign a fixed IP address when the user connects to the L2TP VPN server of the appliance, enter the IP address in the **L2TP Address** field.



Important: Users with a fixed IP address still require a dynamic IP address even though they do not use it. The L2TP VPN Server dynamic IP address range must be large enough to accommodate users with both dynamic and fixed addresses. If IP addresses are in short supply, the unused dynamic IP addresses can be used for other purposes.

- [Model SG565 only] To grant users access to defined printers and storage devices as defined in the Share page, select the **Shares Access** check box.
 - [Conditional. Required if the **Require User Authentication** check box is selected in the Access Control page.] To provide the user with the authority to connect to the Internet, subject to the restrictions defined on the Access Control page, select the **Internet access via access controls** check box. This should be the only option selected for the user for accurate access control tracking. For information on access control, see “Access control” on page 297.
- 9 [Optional] To provide a user with the authority to connect to the Internet as an exemption to the restrictions defined on the Access Control Content Filtering page, select the **Bypass Content Filtering** check box. For further information, see “Access control” on page 297.
- 10 [Optional] To provide the user with the ability to change their password via the Web management console, select the **Change Password** check box.
- 11 Click **Finish**.

Editing a local user

- 1 Click **System > Users > Local Users** tab. The Local Users page is displayed.
- 2 Click the edit icon next to their username. The Edit User Information page is displayed. Make your changes and click **Finish**.

Deleting a local user

- 1 Click **System > Users > Local Users** tab. The Local Users page is displayed.
- 2 Click the delete icon next to their username.
- 3 Confirm the delete. The user is deleted from the list of users.

RADIUS page

The SnapGear appliance can be configured to access a central repository of users and passwords on a RADIUS server to authenticate dial-in, PPTP VPN server, and L2TP VPN server connections. RADIUS can also be used for Wifi 802.1x authentication (SG565 model only).

- 1 From the **System** menu, click **Users > RADIUS** tab. The RADIUS Server page appears.

Figure 362:
RADIUS Server page

RADIUS Configuration

Administrative Users Local Users **RADIUS** TACACS+

RADIUS Test RADIUS

RADIUS Server

RADIUS Server

RADIUS Server Port

RADIUS Secret

Confirm RADIUS Secret

Submit

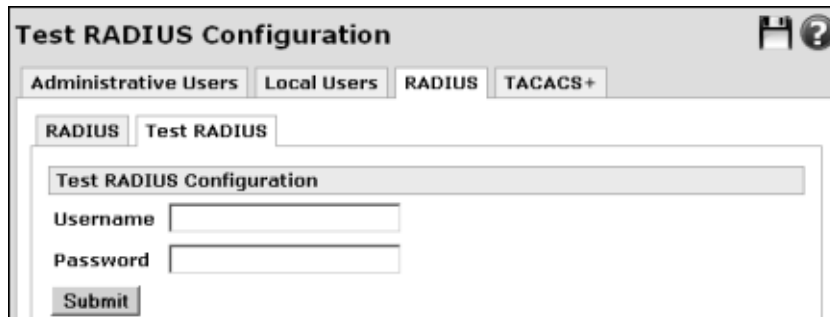
- 2 Enter the **RADIUS Server** address from which to obtain client authentication information.
- 3 Enter a port number in the **RADIUS Server Port** field.
 - Default: 1812. Some older RADIUS servers use port 1645.
 - Range: 1-65535.
- 4 Enter and confirm a secret string in the **RADIUS Secret** field. The secret is used to access the RADIUS server, and can be 1 or more characters of any type.
- 5 Click **Submit**. Now you should test the server. See “Testing the RADIUS server” on page 484.

Testing the RADIUS server

After you configure the RADIUS server, test the configuration.

- 1 From the **System** menu, click **Users > Test RADIUS** tab. The Test RADIUS Configuration page appears.

Figure 363:
Test RADIUS tab



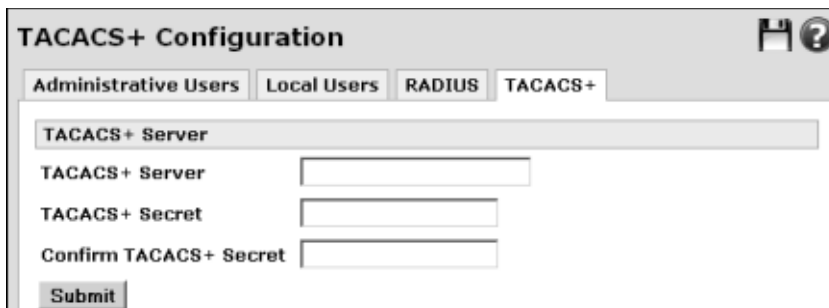
- 2 Enter the user name and password of a valid user in the **Username** and **Password** fields.
- 3 Click **Submit**. A RADIUS request is sent to the server and the result are displayed.
 - If no response is received, carefully check the IP address of the RADIUS server and also the shared secret configuration for this appliance.
 - This test uses a simple PAP request. If your RADIUS server is configured only for CHAP, you may receive an Access Denied message, even for a valid user name/password combination. This is expected behavior.

TACACS+ page

The SnapGear appliance can be configured to access a central repository of users and passwords on a TACACS+ server to authenticate dial-in, PPTP VPN server, and L2TP VPN server connections.

- 1 From the **System** menu, click **Users > TACAS+** tab. The TACACS+ Server page appears.

Figure 364:
TACACS+ Configuration
page



- 2 Enter the address from which to obtain client authentication information in the **TACACS+ Server** field. This address can be a fully qualified domain name of the form *host.domain.com*. Each label (such as host or domain) can consist of alphanumeric characters including hyphens. Each label cannot begin or end with the hyphen (-) character. The address can also be an IP address of the form *a.b.c.d*.
- 3 Enter the secret used to access the TACACS+ server in the **TACACS+ Secret** field. The secret can be 1 or more characters of any type.
- 4 Enter the secret again in the **Confirm TACACS+ Secret** field.
- 5 Click **Submit**.

Management menu

The SnapGear appliance can be managed remotely using the Secure Computing CommandCenter, the legacy Secure Computing CMS (Centralized Management Server), or SNMP (Simple Network Management Protocol).

Note: *If you have Intrusion Detection enabled and configured, and want to use the Management features, you must manually delete the snmp entry in the IDB > UDP port list. For more information, see “Intrusion Detection Systems” on page 284.*

Configuring CommandCenter management

Use this procedure to enable and configure remote management of a SnapGear appliance by a Secure Computing CommandCenter server.

Tip: *Enable the CommandCenter Debug Logging to assist with configuring the CommandCenter. See “Enabling CommandCenter Debug Logging” on page 488.*

Prerequisites:

- The clocks between the appliance and the CommandCenter server must be synced. Make sure the appliance device clock is accurate. See “Date and Time menu” on page 462.
- The time zones must be relatively close (within an hour) between the appliance and the CommandCenter server. Make sure you have selected the correct timezone and that the UTC time is correct.

Note: *Ensure that you have network access and have the CommandCenter server configured appropriately before enabling central management.*

- 1 From the **System** menu, click **Management**. The CommandCenter Management Configuration page appears.

Figure 365:
CommandCenter
Management

CommandCenter Management

CommandCenter Management CMS Management SNMP

CommandCenter Configuration CommandCenter Logging

CommandCenter Management Configuration

This page is used to configure your device for centralized management via CommandCenter.

Enable Central Management ☐

Server Host Name

Server IP Address

Secondary Host Name

Secondary IP Address

Submit Enroll Rapid Deploy

- 2 Select the **Enable Central Management** check box.
- 3 Enter the server host in the **Server Host Name** field. Can be an FQDN (Fully Qualified Domain Name) of the form 'host.domain.com'. Each label ('host' or 'domain') can consist of alphabetic, numeric, or hyphen '-' characters. Each label must not begin or end with the '-' character.
- 4 [Optional] Enter the CommandCenter **Server IP Address**. This can be left blank if you want to use DNS name resolution to connect to the CommandCenter server. The IP address form can be of the format a.b.c.d.
- 5 [Optional] If you have a secondary CommandCenter server, enter its name in **Secondary Host Name** so the SnapGear appliance's firewall can be updated appropriately.
- 6 [Optional] Enter the IP address of the secondary CommandCenter server in **Secondary IP Address** if applicable.
- 7 Choose an option to complete the page:
 - If you are simply changing the IP address of the CommandCenter server, changing secondary server details, or are enabling or disabling a configuration, click **Submit**. A certificate from the CommandCenter server is requested. With the appropriate credentials, you are able to download the appropriate certificates enabling the management of this appliance.
 - If you are registering an appliance with the CommandCenter server, click **Enroll** and go to step 8.
 - To make use of the bulk enrollment provided by the Rapid Deployment feature, click **Rapid Deploy** and go to step 9.
- 8 To register this appliance with the CommandCenter server using the standard mechanism, click **Enroll**. You are challenged for a password.
 - a Click the [here](#) link. A Web page from the CommandCenter appears. Copy and paste the challenge password.

- 1** From the **System** menu, click **Management > CommandCenter Logging** tab. The CommandCenter Management Logging page appears.
- 2** Clear the **Enable Debug Log** check box.
- 3** Click **Update**.

Enabling remote management by CMS

Use this procedure to enable remote management by a Secure Computing CMS (Central Management Server).

Note: CMS is a legacy feature that is no longer a product offering. The documentation for the feature is provided for customers who still use the feature.

- 1 From the **System** menu, click **Management > CMS Management** tab. The Centralized Management Settings page appears.

Figure 367: Centralized Management Settings

Centralized Management Settings

CommandCenter Management CMS Management SNMP

CMS Management CMS Attributes

Centralized Management Configuration

These settings are used to allow this device to be managed by the Central Management Server. Enter the values assigned by your central system administrator. The authentication key must be entered EXACTLY in order for management communication to be established.

Enable Central Management ☐

IP Address of CMS

Authentication Key

Back-to-base ping interval (s)

Local SNMP port

SNMP trap port on CMS

Administrative Contact

Device Location

Syslog Remote Port

Syslog Filter

Submit

- 2 Select the **Enable Central Management** check box.
- 3 In the **IP Address of CMS** field, enter the IP address of the host on which the CMS is running.
- 4 In the **Authentication Key** field, specify the shared key with which to authenticate the appliance against the CMS. This key must be the same as the `snmp_community` configuration setting for CMS.
 - 1 or more characters of any type
- 5 In the **Back-to-base ping interval(s)** field, specify the interval in seconds between these pings. The appliance periodically sends a ping (SNMP trap) back to the CMS to indicate it is alive. This interval must be less than the `max_alive_interval` configuration setting for CMS.

- Default: 300
- 6** In the **Local SNMP Port** field, specify the port on which the management agent listens for requests. If you change the port, it must be an unused UDP port.
- Default: 161
 - Can be a space-separated list of endpoints



Important: If you enabled the SNMP agent under **Management > SNMP** (see “Enabling the SNMP agent” on page 495), change the Local SNMP Port in this CMS page.

- 7** In the **SNMP trap port on CMS** field, specify the CMS UDP port to send SNMP traps to. This must be the same as the `snmp_trapport` configuration setting for CMS.
- Default: 162
 - Range: 1-65535
- 8** [Optional] Enter the contact information of the local administrator in the **Administrative Contact** field, which is the SNMP `sysContact` field.
- 9** [Optional] Enter a short description of the physical location of the device in the **Device Location** field, which is the SNMP `sysLocation` field.
- 10** Enter the **Syslog Remote Port** to which to send syslog messages. This must be the same as the `syslog_port` configuration setting for CMS.
- Default: 514
 - Can be an integer equal to or greater than 1
- 11** Select a logging level from the **Syslog Filter** list. The setting filters syslog messages sent to CMS. Typically, a setting somewhere between the logging everything and nothing is appropriate. Available options are:
- **Absolutely Everything**—Most verbose setting that sends all messages, including debug messages. This may result in excessive messages being sent to CMS.
 - **Everything but Debug**
 - **Notices, Warnings, and Errors**
 - **Errors and Warnings**
 - **All Error Conditions**
 - **Emergency, Alerts, and Critical Errors**
 - **Emergency and Alerts Errors**
 - **Emergency Errors only**
 - **Log Nothing**—Sends no messages, which can make troubleshooting more difficult.
- 12** Click **Submit**.

Disabling CMS

- 1** From the **System** menu, click **Management > CMS Management** tab. The Centralized Management Settings page appears.
- 2** Clear the **Enable Central Management** check box.
- 3** Click **Submit**.

CMS Attributes

The CMS allows devices to be categorized according to user-defined attributes. You can add, edit, and delete device attributes.

Creating a CMS attribute

- 1 From the **System** menu, click **Management > CMS Management > CMS Attributes** tab. The CMS Attributes page appears.

Figure 368: CMS Attributes

- 2 Click **New**. The Edit CMS Device Attributes page appears.

Figure 369: Edit CMS Device Attributes

- 3 Enter a name in the **Attribute Name** field. The name must begin with an alpha character.
- 4 [Optional] Enter a value in the **Attribute Value** field.
- 5 Click **Finish**. The device attribute is displayed in the attributes list.

Figure 370: CMS Device Attributes edit list

Editing a CMS attribute

- 1 From the **System** menu, click **Management > CMS Management > CMS Attributes** tab. The CMS Attributes page appears.
- 2 Click the edit icon for the attribute you want to edit. The Edit CMS Device Attributes page appears.
- 3 Make your changes and click **Finish**.

Deleting a CMS attribute

- 1 From the **System** menu, click **Management > CMS Management > CMS Attributes** tab. The CMS Attributes page appears.
- 2 Click the delete icon for the attribute you want to delete. You are prompted to confirm the delete.
- 3 Click **OK**.

Enabling the SNMP agent

Use this procedure to enable and configure the SNMP agent. The SNMP agent allows external SNMP management software to query the appliance for management information.

- 1 From the **System** menu, click **Management > SNMP** tab. The SNMP Agent Configuration page appears.

Figure 371: SNMP Agent

- 2 Select the **Enable SNMP Agent** check box.
- 3 [Optional] Enter the name of a community that is allowed read-only access in the **Read-Only Community** field. You can optionally include an IP address or network to restrict who is allowed access. You can optionally include an OID (Object Identifier) to restrict the fields that are accessible.
- 4 [Optional] Enter the name of a community that is allowed read-write access in the **Read-Write Community** field. You can optionally include an IP address or network to restrict who is allowed access. You can optionally include an OID to restrict the fields that are accessible.



Caution: The community name is equivalent to a password, and is sent in plain text in every SNMP packet. Anyone who knows the community name is able to modify settings on this device. It is highly recommended you do not allow read-write access; otherwise, take additional steps to secure the connection.

- 5 Specify the endpoints on which the SNMP agent accepts requests in the **Local SNMP Port** field. An endpoint consists of an optional transport, an optional address, and a port that is separated by colon (:) characters. The default transport is UDP, and the default address is any address. The field can contain a space-separated list of endpoints.
 - Examples: **1161**, **tcp:161**, **10.0.0.1:1161**, or **tcp:10.0.0.1:1161**.
 - Default: Port 161

- 6 [Optional] The **Administrative Contact** is the SNMP *sysContact* field. Any value can be specified, but a good choice is contact information for the local administrator.
- 7 [Optional] The **Device Location** is the SNMP *sysLocation* field. Any value can be specified. A short description of the physical location of the device is recommended.
- 8 Click **Submit**.

Disabling the SNMP agent

- 1 From the **System** menu, click **Management > SNMP** tab. The SNMP Agent Configuration page appears.
- 2 Clear the **Enable SNMP Agent** check box.
- 3 Click **Submit**.

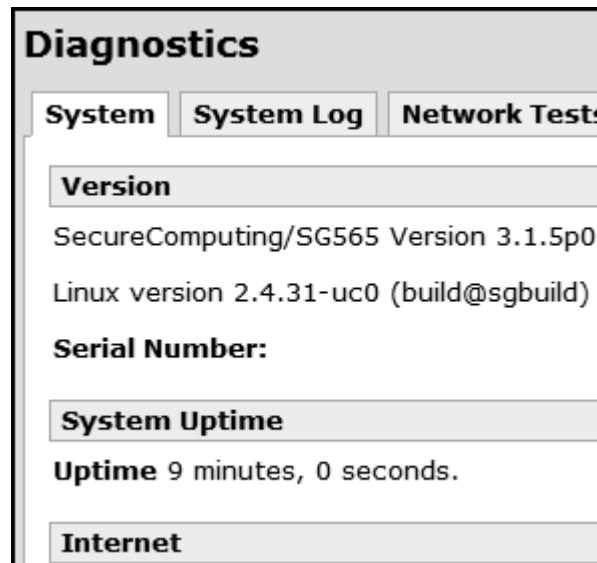
Diagnostics menu

Low-level diagnostic information and network tests are provided to assist you in diagnosing network problems.

System tab

The System page displays information including the current firmware version, serial number, network settings, and the status of Internet and VPN connections.

Figure 372: System tab



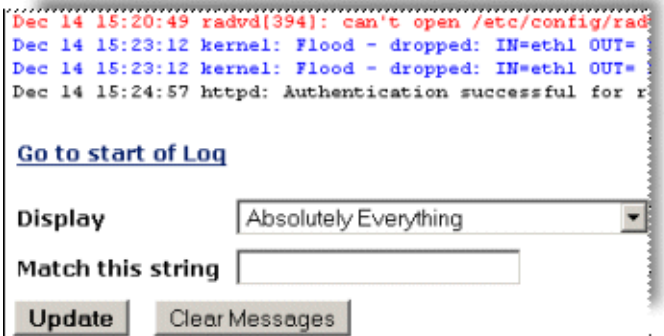
- 1 From the **System** menu, click **Diagnostics**. The System tab appears.
- 2 Scroll the file to view the available information.

Viewing the Local System Log

The system log contains debugging information that may be useful in determining whether all services for your SnapGear appliance are operating correctly. Every message recorded by a service on the appliance has an associated logging level such as “Debug” or “Warning”. By default, all log level messages are posted to the System Log. You can filter the displayed messages or reset the default filtering level. The Local System Log is stored in the `/var/log/messages` directory. The appliance rotates and ages the messages file. Only one copy of the file is kept in the directory.

Log output is color-coded by output type. General information and debug output is **black**, warnings and notices are **blue**, and errors are **red**.

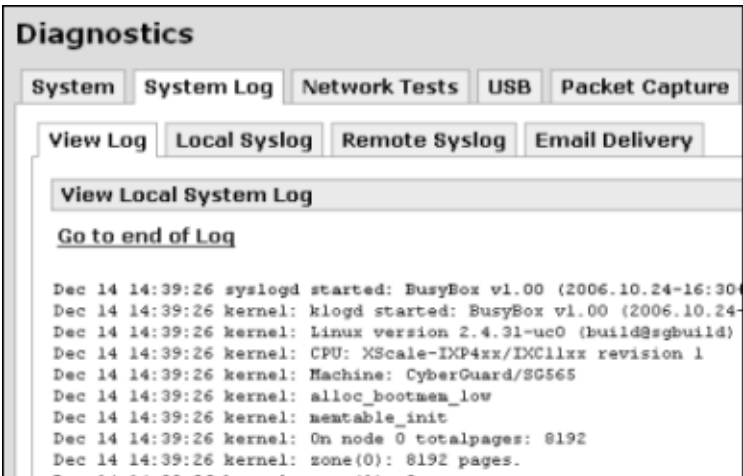
Figure 373: Color-coded Log output



To open and navigate the System Log

- 1 From the **System** menu, click **Diagnostics > System Log** tab. The View Local System Log page appears.

Figure 374: View System Log



- 2 Within this log, you can do the following:
 - Click **Go to end of Log** link to go to the end of the log.
 - Click **Go to start of Log** link to go return to the top.
 - To search for a string, enter characters in the **Match this string** field and click **Update**. The log isolates your search terms.
 - To clear the system log messages, click **Clear Messages**.
 - To filter the log output to display based on output type, select an option from the **Display** list. To reset the default filtering level, see Configuring local system log settings.

For details on interpreting log output and configuring advanced log rules, refer to Appendix A, System Log.

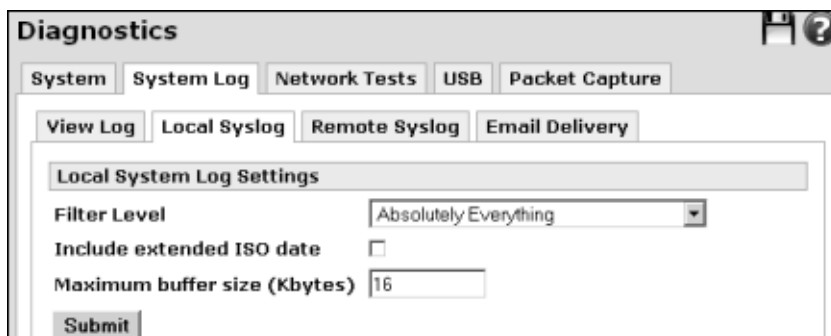
Configuring local system log settings

By default, all messages are recorded in the System Log. The Filter Level setting allows you to control which classes of messages are recorded in the system log.

Tip: If your logging requirements generate extremely large log sizes, Secure Computing recommends using a remote syslog server. See “Enabling remote system logging” on page 501.

- 1 From the **System** menu, click **Diagnostics > System Log tab > Local Syslog** tab. The Local System Log Settings page appears.

Figure 375: System Log Settings



The screenshot shows the 'Diagnostics' menu with tabs for 'System', 'System Log', 'Network Tests', 'USB', and 'Packet Capture'. The 'System Log' tab is selected, and within it, the 'Local Syslog' sub-tab is active. The 'Local System Log Settings' section contains the following controls:

- Filter Level:** A dropdown menu currently set to 'Absolutely Everything'.
- Include extended ISO date:** An unchecked checkbox.
- Maximum buffer size (Kbytes):** A text input field containing the value '16'.
- Submit:** A button at the bottom of the settings section.

- 2 Select a default filtering level from the **Filter Level** list. Available options include:
- Absolutely Everything (most verbose)
 - Everything but Debug
 - Notices, Warnings, and Errors
 - Errors and Warnings
 - All Error Conditions
 - Emergency, Alerts, and Critical Errors
 - Emergency and Alerts Errors
 - Emergency Errors only (least verbose)
- 3 [Optional] Every message recorded in the System Log includes a basic time stamp. To force a more precise and standardized time stamp with every message, select the **Include extended ISO date** check box.
- 4 To increase the size of this buffer to retain more messages when tracking down issues, enter an increased integer value in the **Maximum buffer size** field. This field specifies the maximum size of the local buffer that contains syslog messages.



Caution: Make sure the value you enter does not exceed the maximum size of the `/var/log` filesystem available for your model as indicated in Table 22, “Temporary storage space by model (`/var/log`)”. For best results, keep the log size approximately half the size of the available space to accommodate rotating system logs.

- 5 Click **Submit**.

Table 22: Temporary storage space by model (`/var/log`)

Models	Maximum size
SG720	This model have a dynamic <code>/var</code> filesystem size with a maximum size of 128 MB. This space is possibly shared with Web cache and antivirus if enabled.
SG565, SG580, SG640	These models have a dynamic <code>/var</code> filesystem size with a maximum size of 33 MB. This space is possibly shared with Web cache and antivirus if enabled.
SG560	512 K fixed size.
SG300	128 K fixed size.

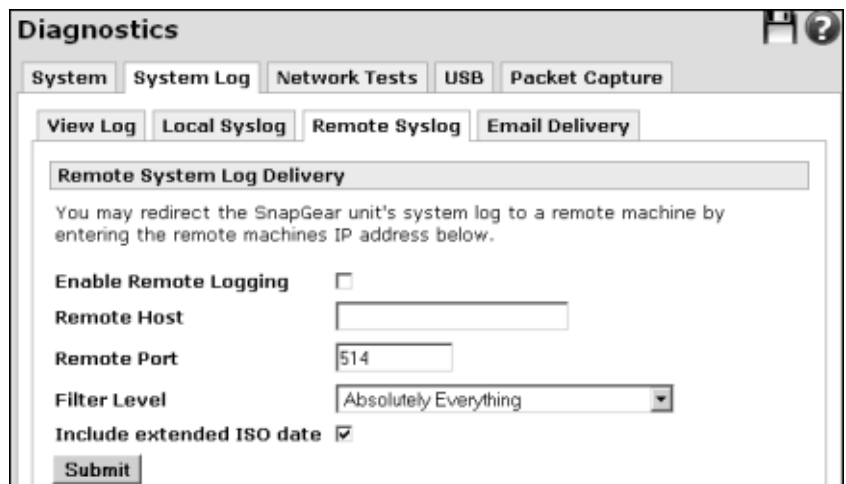
Enabling remote system logging

Use this procedure to redirect the system log messages to a remote system. System log messages can be sent to a remote syslog server, which allows you to keep system log messages persistently.

Tip: There are freely available syslog servers for the Windows platform. For more information, refer to the SnapGear KB article #2722 in <http://sgkb.securecomputing.com>

- 1 From the **System** menu, click **Diagnostics > System Log tab > Remote Syslog** tab. The Remote System Log Delivery page appears.

Figure 376: Remote System Log Delivery

The screenshot shows a web-based configuration interface titled "Diagnostics". It has a top navigation bar with tabs: "System", "System Log", "Network Tests", "USB", and "Packet Capture". Below this is a sub-navigation bar with tabs: "View Log", "Local Syslog", "Remote Syslog", and "Email Delivery". The "Remote Syslog" tab is selected. The main content area is titled "Remote System Log Delivery" and contains the following text: "You may redirect the SnapGear unit's system log to a remote machine by entering the remote machines IP address below." Below this text are four configuration fields: "Enable Remote Logging" with an unchecked checkbox, "Remote Host" with an empty text input field, "Remote Port" with a text input field containing "514", and "Filter Level" with a dropdown menu showing "Absolutely Everything". At the bottom, there is a checkbox for "Include extended ISO date" which is checked, and a "Submit" button.

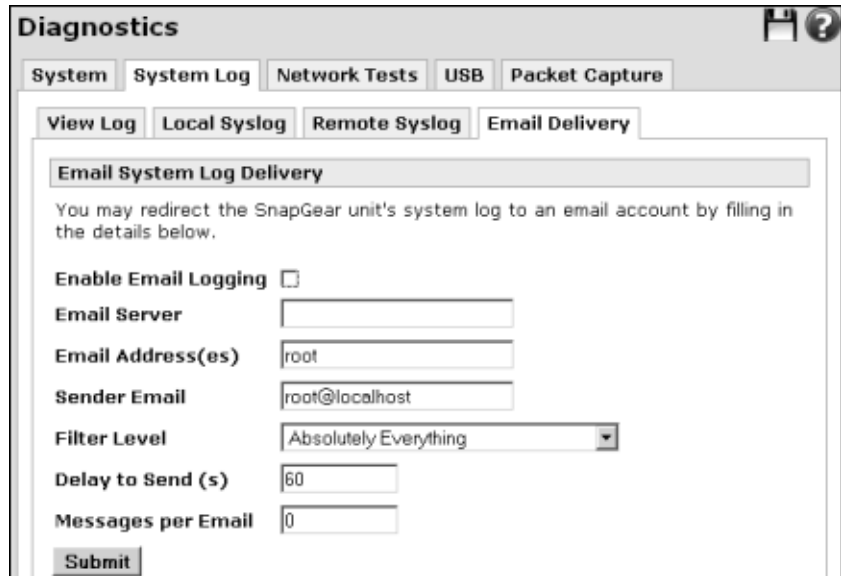
- 2 Select the **Enable Remote Logging** check box.
- 3 Enter the IP address or DNS hostname for the remote syslog server in the **Remote Host** field.
- 4 Enter the **Remote Port** on which the remote syslog server is listening for syslog messages. Typically, the default is correct.
- 5 Set the **Filter Level** to only send syslog messages at this level or above.
- 6 [Optional] To force a more precise and standardized time stamp with every message, select the **Include extended ISO date** check box. The date is prepended to syslog messages before being sent.
- 7 Click **Submit**.

Sending log messages to an email account

Use this procedure to reroute the system log messages to an email account. Syslog log messages can be sent to an email account, which allows you to keep system log messages persistently.

- 1 From the **Diagnostics** menu, click **System Log** tab > **Email Delivery** tab. The Email System Log Delivery page appears.

Figure 377: Email System Log Delivery page



The screenshot shows the 'Diagnostics' menu with tabs for 'System', 'System Log', 'Network Tests', 'USB', and 'Packet Capture'. The 'System Log' tab is selected, and within it, the 'Email Delivery' sub-tab is active. The page title is 'Email System Log Delivery'. Below the title, a message states: 'You may redirect the SnapGear unit's system log to an email account by filling in the details below.' The configuration fields include: 'Enable Email Logging' (unchecked checkbox), 'Email Server' (empty text box), 'Email Address(es)' (text box containing 'root'), 'Sender Email' (text box containing 'root@localhost'), 'Filter Level' (dropdown menu set to 'Absolutely Everything'), 'Delay to Send (s)' (text box containing '60'), and 'Messages per Email' (text box containing '0'). A 'Submit' button is at the bottom.

- 2 Select the **Enable Email Logging** check box.
- 3 Enter the address of an **Email Server** (SMTP server) that accepts email for forwarding.
- 4 Enter the **Email Address(es)** to which to send the system log messages.
- 5 Specify the **Sender Email** address that System Log messages are sent from.
- 6 Set the **Filter Level** to only send syslog messages at the selected level or above.
- 7 Specify the number of seconds to wait after receiving a system log message before sending an email in **Delay to Send(s)**. This allows multiple system log messages to accumulate before sending an email containing all messages.
- 8 **Messages per Email** is the maximum number of system log messages that are allowed to accumulate before sending the email. The default setting of 0 means unlimited, and is typically appropriate for all systems except those that experience heavy traffic.
- 9 Click **Submit**.

Network Tests page

The basic network tests of ping and traceroute help test the current functionality of the SnapGear appliance.

Figure 378: Ping and Trace Route Tests page

The screenshot shows the 'Diagnostics' menu with tabs for 'System', 'System Log', 'Network Tests', 'USB', and 'Packet Capture'. The 'Network Tests' tab is active. It contains instructions for performing a ping test (entering a remote machine address and pressing 'Ping', with a note that it takes 10-15 seconds) and a traceroute test (entering a remote machine address and pressing 'Traceroute', with a note that it takes a few minutes). Below the instructions are input fields for 'IP Address of Remote Machine' (containing '175.16.1.1') and 'Source Interface' (a dropdown menu showing 'WIFI (Wireless, 172.16.1.1)'). There is also a 'Lookup DNS Names' checkbox which is checked. At the bottom are 'Ping' and 'Traceroute' buttons.

Ping test

Use this procedure to perform a ping test within the Web management console. Use the ping test to verify packets are able to reach and return from a specific host either on the Internet or on your local network.

- 1 From the **System** menu, click **Diagnostics > Network Tests** tab. The Network Tests page appears.
- 2 Enter the IP Address of the box you want to ping in the **IP Address of Remote Machine** field.
- 3 [Optional] Select an interface from the **Source Interface** list.
 - Default: None.

***Tip:** If you are trying to ping the remote end of an IPSec tunnel, use the LAN interface of the appliance where the LAN network is defined as the local network. Otherwise, the ping will fail.*

- 4 [Optional] To perform a reverse DNS names lookup on IP addresses, select the **Lookup DNS Names** check box.
- 5 Click **Ping**.

The results of the test are displayed.

Figure 379: Ping test results

System	System Log	Network Tests	USB	Packet Capture
Action Successful				
The following results were returned:				
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.				
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.515 ms				
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.433 ms				
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=0.436 ms				
64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=0.430 ms				

192.168.0.1 ping statistics ---				
4 packets transmitted, 4 received, 0% packet loss, time 3025ms				
rtt min/avg/max/mdev = 0.430/0.453/0.515/0.041 ms				

Traceroute test

Use this procedure to perform a traceroute test within the Web management console. The Traceroute test traces the network path that packets travel as they attempt to reach and return from a specific host either on the Internet or on your local network.

Note: Since the SnapGear appliance runs on the Linux OS, it uses UDP probes in traceroute by default. This is in contrast to the Windows platform, which uses ICMP. Depending on what is blocked upstream, you may observe different results between platforms.

- 1 From the **System** menu, click **Diagnostics > Network Tests** tab. The Network Tests page appears.
- 2 Enter the IP Address of the box you want to trace packet routing for in the **IP Address of Remote Machine** field.
- 3 [Optional] Select an interface from the **Source Interface** list.
 - Default: None.
- 4 [Optional] To perform a reverse DNS names lookup on IP addresses, select the **Lookup DNS Names** check box.
- 5 Click **Traceroute**. The results of the test are displayed.

Figure 380: Trace route results

System	System Log	Network Tests	USB	Packet Capture
Action Successful				
The following results were returned:				
traceroute to 172.16.1.1 (172.16.1.1), 30 hops max, 40 byte packets				
1 172.16.1.1 (172.16.1.1) 1 ms 0 ms 1 ms				

Detected USB Devices

Use this procedure to display the current Universal Serial Bus devices plugged in and detected by the appliance.

Note: USB is available on the SG565 model only.

For more information about USB devices, see Chapter 6, USB.

From the **System** menu, click **Diagnostics > USB** tab. The USB Devices page appears.

Figure 381: USB
Detected Devices



The **Vendor**, **Product** and **ID** details are obtained by querying the devices directly. The **ID** field is a combination of the **Product ID**, **Vendor ID**, and **Serial Number**. If this is missing, or the same as any other devices, then configuring and using the device may be unreliable.

The **Driver** field shows the driver module loaded to utilize the USB device. If this is listed as (None), then the appropriate sub-system may not be currently enabled or the driver may need to be manually loaded. Refer to the Technical Support Knowledge Base for a list of what devices are supported, and how to manually load drivers for devices that are not automatically detected.

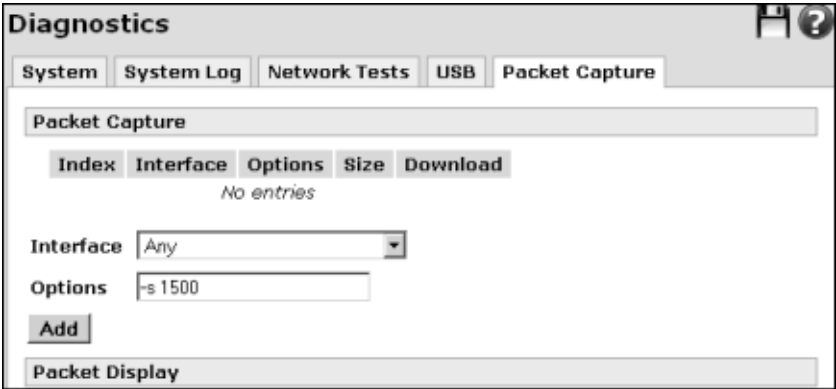
Packet Capture page

You can capture network traffic in a packet capture (*pcap*) file. Packet captures are saved to *n.pcap* files in the */var/tmp* directory. You can either download or decode the *.pcap* file. This can be useful for diagnosing network problems. The downloaded file can also be viewed using freely available utilities such as tcpdump or Wireshark.

Capturing and displaying packets

- 1 From the **System** menu, click **Diagnostics > Packet Capture**. The Packet Capture page appears.

Figure 382: Packet Capture page



- 2 Select the interface on which you want to capture packets from the **Interface** list.
- 3 [Optional] Adjust the packet size if necessary in the **Options** field. The default packet capture size is 1500 bytes, and is entered as **-s 1500**. This guarantees that the packet is fully captured and can be fully decoded. However, for large packet captures, this size will quickly consume the temporary storage available on the appliance. For further information on temporary storage space, see Table 22 on page 500. For large packet captures, decrease this value.

- 4 Click **Add**. The packet capture configuration is added to the Index list.

Figure 383: Packet Capture added and indexed

The screenshot shows the 'Diagnostics' window with the 'Packet Capture' tab selected. The 'Packet Capture' section contains a table with one entry:

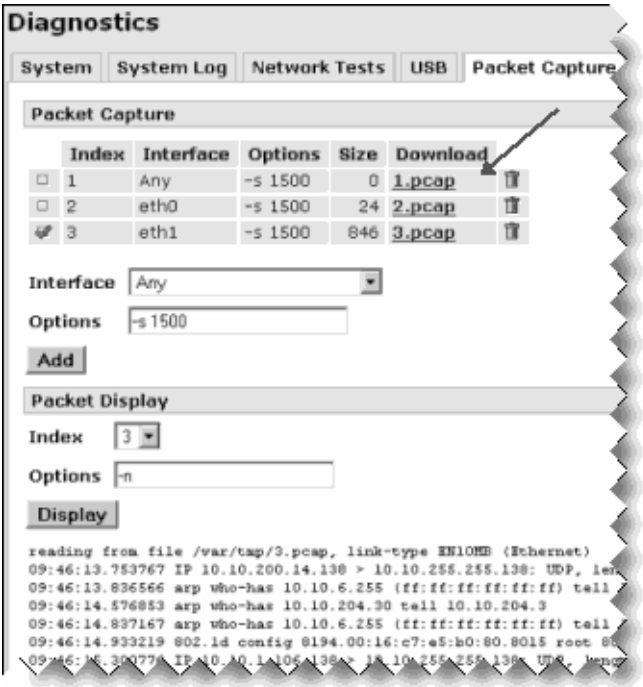
Index	Interface	Options	Size	Download
<input type="checkbox"/> 1	Any	-s 1500	0	1.pcap

Below the table, the 'Interface' is set to 'Any' and 'Options' is set to '-s 1500'. An 'Add' button is visible. The 'Packet Display' section shows 'Index' set to '1' and 'Options' set to '-n', with a 'Display' button.

- 5 Click the check box next to the definition **Index** number to enable the packet capture.
- 6 Perform the network operation that you wish to capture.
- 7 Disable the packet capture by clicking on the check box again.
- 8 Select the packet capture configuration you want to display from the **Index** list.
- 9 [Optional] If desired, adjust the default display options in the **Options** field. The default packet display option is '-n', which disables DNS lookups for IP addresses. For some examples, see "More filtering options" on page 509.

10 Click **Display** to decode and display the packets in the Packet Capture page.

Figure 384: Packet Capture Display



Downloading a pcap file

Use this procedure to download the .pcap file for examination rather than viewing it within the Packet Capture page.

- 1 From the **System** menu, click **Diagnostics > Packet Capture**. The Packet Capture page appears.
- 2 Click the pcap file link in the **Download** column to download the *n.pcap* file.
- 3 You are prompted to save the downloaded file.

Disabling a pcap file

- 1 From the **System** menu, click **Diagnostics > Packet Capture**. The Packet Capture page appears.
- 2 Clear the enabled check box for the .pcap file. The page refreshes and a check mark is no longer displayed in the enable check box.

Deleting a pcap file

Use this procedure to delete pcap files when you no longer require them. This keeps space available in the `/var/tmp` directory.

- 1 From the **System** menu, click **Diagnostics > Packet Capture**. The Packet Capture page appears.
- 2 Click the delete icon next to the `.pcap` file you want to delete. The file is deleted.

More filtering options

You can specify filtering options during both capture and display which restrict the packets that are captured or displayed. For full documentation of these options, see the tcpdump project at:

<http://sourceforge.net/projects/tcpdump/>

Some common filtering options are shown in the examples in Table 23 below:

Table 23: Filtering options for packets

Packet Filtering Option	Description
<code>host 1.2.3.4</code>	Match packets with a source or destination IP address of 1.2.3.4.
<code>src host 1.2.3.4</code>	Match packets with a source IP address of 1.2.3.4.
<code>dst host 1.2.3.4</code>	Match packets with a destination IP address of 1.2.3.4.
<code>ether host aa:bb:cc:dd:ee:ff</code>	Match packets with an Ethernet source or destination address of aa:bb:cc:dd:ee:ff.
<code>ether src aa:bb:cc:dd:ee:ff</code>	Match packets with an Ethernet source address of aa:bb:cc:dd:ee:ff.
<code>ether dst aa:bb:cc:dd:ee:ff</code>	Match packets with an Ethernet destination address of aa:bb:cc:dd:ee:ff.
<code>tcp port 80</code>	Match TCP packets with a source or destination port of 80.
<code>tcp src port 80</code>	Match TCP packets with a source port of 80.

Packet Filtering Option	Description
<code>tcp dst port 80</code>	Match TCP packets with a destination port of 80.
<code>udp port 80</code>	Match UDP packets with a source or destination port of 80.
<code>udp src port 80</code>	Match UDP packets with a source port of 80.
<code>udp dst port 80</code>	Match UDP packets with a destination port of 80.
<code>ip proto 1</code>	Match IP packets with a protocol of 1 (ICMP).
<code>option and option</code>	Match packets if both of the options match.
<code>option or option</code>	Match packets if either of the options match.
<code>not option</code>	Invert any of the previous options.

Advanced menu

The advanced menu options are intended for network administrators and advanced users *only*.



Caution: Altering the advanced configuration settings may render your SnapGear appliance inoperable.

Reboot and Reset

Rebooting does not erase your SnapGear appliance's configuration; however, network connections such as your Internet connection and VPN tunnels are terminated and reestablished when the device is up and running again.



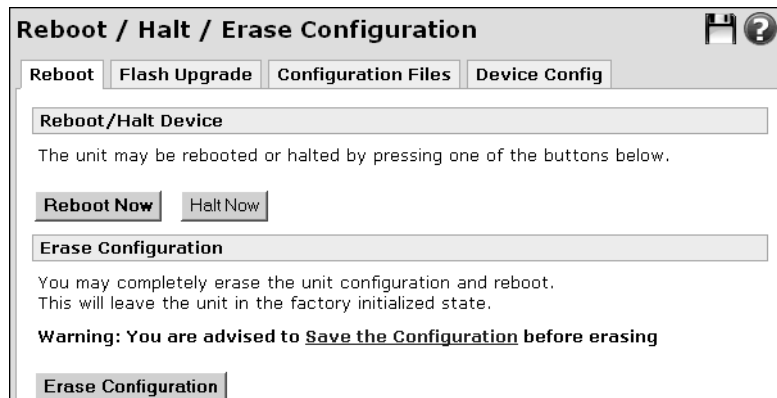
Caution: Before restoring your SnapGear appliance to its default factory settings via the Web management console or erase button, it is strongly recommended that you create a back up of your configuration. See "Backing up a configuration remotely" on page 470.

Soft rebooting the device

Use this procedure to perform a soft reboot of the appliance. Normally, this should not be required, but if so, should be done from the user interface rather than from the command line to prevent configuration from being lost.

- 1 From the **System** menu, click **Advanced**. The Reboot/Halt/Erase Configuration page appears.

Figure 385: Reboot/Halt /Erase Configuration



- 2 Click **Reboot Now**. It usually takes around 10 seconds before the appliance is up and running again. If you have enabled bridging, the SnapGear appliance may take up to 30 seconds to reboot. Any shared printers take 30 seconds to become available, during which time print jobs are not accepted.

Halting the appliance before powering down

Use this procedure to halt the appliance before you power down. This ensures all configuration is saved. If external devices are connected to the appliance, such as USB drives, there may be cached data stored on the appliance. To avoid loss of data, halt the appliance to force an orderly shutdown. Allow the SG300 about two to three seconds to perform a halt; allow other models 20-30 seconds before powering down after a halt.

- 1 From the **System** menu, click **Advanced**. The Reboot/Halt//Erase Configuration page appears.
- 2 To halt the appliance, click **Halt Now**. The H/B (HeartBeat) LED and all other LEDs except for Power turn off. You can now safely power down the appliance.

Erasing configuration and rebooting

Use this procedure to erase the configuration of your SnapGear appliance and return to the factory default settings. This is useful if you want to reconfigure the device from scratch after an upgrade, or want to redeploy the device into a different environment. Be sure to save your current configuration before proceeding.

- 1 From the **System** menu, click **Advanced**. The Reboot/Halt/Erase Configuration page appears.
- 2 Click **Erase Configuration**.

Erase button

Another method to clear the SnapGear appliance's stored configuration information is by pushing the erase button on the back panel of the SnapGear appliance **twice, 1 second apart but within 3 seconds**. Pressing the button too quickly will not erase the appliance.

Tip: *Either use a secondhand on a watch or count “one thousand one, one thousand two, one thousand three”, while pressing the erase button on counts one and three.*

The erase button is particularly useful should the appliance become uncontactable; for example, due to misconfiguration. Pushing the erase button twice as instructed clears all stored configuration information, reverts all settings to the factory defaults, and reboots the SnapGear appliance. When the SnapGear appliance reboots, it has an IP address of 192.168.0.1; netmask 255.255.255.0. The appliance also accepts an assigned IP address if there is a DHCP server on the LAN/A port. You can contact the appliance on either the default or the DHCP-assigned address.

Upgrading firmware

Periodically, Secure Computing releases new versions of firmware for your SnapGear appliance. If a new version fixes an issue you have been experiencing, or contains a new feature you want to use, go to the download page on the product registration Web site to obtain the latest firmware. You can then load the new firmware with a flash upgrade.



Caution: *Before attempting a firmware upgrade, read “Firmware upgrade best practices and precautions” on page 552.*

There are two primary methods available for performing a flash upgrade, Netflash and Flash upgrade via HTTP. Remote upgrades can also be performed using TFTP if you have a TFTP server at the remote site.

During the upgrade, the front panel LEDs on the SnapGear appliance flash in an in-and-out pattern. The appliance retains its configuration information with the new firmware.



Caution: *If the flash upgrade is interrupted (such as powered down), the SnapGear appliance stops functioning and becomes unusable until a recovery boot is performed. User care is advised. For instructions on performing a recovery boot, “Recovering from a failed upgrade” on page 554.*

Upgrading flash firmware via HTTP

Use this procedure to perform a flash upgrade of firmware via HTTP. The SnapGear Firmware Upgrades page is available from the following URL:
<http://www.securecomputing.com/index.cfm?skey=1597>

Note: *This feature is only available on firmware versions 2.1.4 or higher. If you have a lower firmware version, you must use the Netflash executable to perform a flash upgrade. Be sure to read the release notes and important migration notes posted on the firmware download page. If you do not upgrade your firmware to 2.1.4 or higher, you must use the Netflash executable to perform a flash upgrade. See “Upgrading firmware using Netflash” on page 553.*

Prerequisites:

- Download the binary image file (.sgu).
- Backup your current configuration if you have not already done so. See “Backing up a configuration remotely” on page 470.

Figure 386: Flash Upgrade (HTTP) page

Flash Upgrade (HTTP)

Reboot Flash Upgrade Configuration Files Device Config

Upgrade via HTTP Upgrade via TFTP

Information Regarding Flash Upgrade

Warning: Should the flash upgrade be interrupted in any manner (such as removing power) the SnapGear unit will stop functioning and will be unusable until its flash is reprogrammed using the recovery procedure. User care is recommended in completing this step.

Warning: Ensure that before upgrading firmware you have created an encrypted version of your configuration and stored it in a safe place. This can be done on the [Store/Restore](#) page.

It may take a minute for the web page to appear after you have started this step.

Note: When you click the Upgrade button below, the SnapGear unit will stop responding while it downloads the new image.

Flash Upgrade via HTTP

Select the image file from your local file system that you wish to use to upgrade the unit. The file will be transferred to the unit via your web-browser.

Note, SnapGear upgrade image names take the form of MODEL_VERSION_DATE.sgu (e.g. SG550_v2.0.2_20040621.sgu).

Local Filename Browse...

Warning: Put extra parameters in here at the request of customer support only.

Extra Parameters

Upgrade

To upgrade your firmware using flash upgrade HTTP

- 1 From the **System** menu, click **Advanced > Flash Upgrade** tab. The Flash Upgrade via HTTP page appears.
- 2 Click **Browse** to locate the .sgu file on your local PC.
- 3 Enter any **Extra Parameters** only at the request of Secure Computing technical support staff.

Tip: Should you require to downgrade your firmware or restore a configuration from an earlier firmware version, enter **-i** in the Extra Parameters field to circumvent the firmware version checking.

- 4 Click **Upgrade**. Wait for the upgrade to complete.

Upgrading flash firmware via TFTP

Trivial File Transfer Protocol (TFTP) is a simplified version of FTP that allows transfer of files between computers over a network. An alternative method to flash upgrades via HTTP is to install and configure a TFTP server and use that for flash upgrades. The majority of Linux distributions include a TFTP server; Windows users can download one from:

<http://www.snapgear.com/ftp/tools/tftpd32j.zip>

Note: *Although TFTP is an option for upgrading, this program is not supported by Secure Computing technical support.*

Prerequisites:

- Download the binary image file (.sgu). Go to the product Web site for instructions on obtaining this file. The SnapGear Firmware Upgrades page is available from the following URL:

<http://www.securecomputing.com/index.cfm?skey=1597>

- Place the .sgu file in the directory your TFTP is serving files from, usually: `/tftpboot/`.

To flash upgrade with TFTP, you can either use the Flash Upgrade (TFTP) page or run a command on the command line interface.

Upgrading TFTP from the Web management console

Prerequisites:

- Download the binary image file (.sgu) and place it on the machine running the TFTP server.
- Backup your current configuration if you have not already done so. See “Backing up a configuration remotely” on page 470.

Figure 387: Flash Upgrade via TFTP

Flash Upgrade (TFTP)

Reboot | **Flash Upgrade** | Configuration Files | Device Config

Upgrade via HTTP | **Upgrade via TFTP**

Information Regarding Flash Upgrade

Warning: Should the flash upgrade be interrupted in any manner (such as removing power) the SnapGear unit will stop functioning and will be unusable until its flash is reprogrammed using the recovery procedure. User care is recommended in completing this step.

Warning: Ensure that before upgrading firmware you have created an encrypted version of your configuration and stored it in a safe place. This can be done on the [Store/Restore](#) page.

It may take a minute for the web page to appear after you have started this step.

Note: When you click the Upgrade button below, the SnapGear unit will stop responding while it downloads the new image.

Flash Upgrade via TFTP

Type in the IP address of the machine that is running a TFTP server and that also has the upgrade image file. You will also need to specify the file's correct name.

Note, SnapGear upgrade image names take the form of `MODEL_VERSION_DATE.sgu` (e.g. `SG550_v2.0.2_20040621.sgu`).

IP Address

Filename

Warning: Put extra parameters in here at the request of customer support only.

Extra Parameters

Upgrade

To upgrade firmware using the TFTP page

- 1 From the **System** menu, click **Advanced** > **Flash Upgrade** tab > **Flash Upgrade via TFTP** tab. The Upgrade via TFTP page appears.
- 2 Enter the IP address of the machine running the TFTP server in the **IP address** field.

- 3 Enter the name of the image file in the **Filename** field. Place this file in the directory your TFTP is serving files from, usually: */tftpboot/*.
- 4 Enter any **Extra Parameters** *only* at the request of Secure Computing technical support staff.
- 5 Click **Upgrade**. The firmware upload only accepts valid firmware images and only accepts newer images appropriate for your device. Wait for the upgrade to complete.

Upgrading flash using TFTP on the command line interface

Use this procedure to perform a flash upgrade using TFTP on the command line interface.

Note: *The Web management console provides the same functionality as the command line interface for flash upgrades via TFTP. Using the command line for flash upgrades is only recommended if the upgrade from the Web management console TFTP page is failing, and you want additional diagnostic information.*

- 1 Establish a telnet or ssh connection to the SnapGear appliance.
- 2 Login and run the command:
`netflash <TFTP server address> <image.sgu>`
.. where *<TFTP server address>* is the address of your TFTP server, and *<image.sgu>* is the binary image filename. Your telnet or ssh connection is terminated once the upgrade commences.

Configuration Files tab

The Configuration Files tab provides direct and quick access to configuration files within the Edit Files subtab.

The **Filename** column indicates the configuration file name. The **Size** column indicates the amount of space on the configuration that a file is using. There is a limited amount of configuration space available on an appliance. The **Mode** column indicates whether a file has read (r), write (w), and delete (x) access.



Caution: Exercise caution when manually editing configuration files. Manually modifying or deleting the configuration files of your SnapGear appliance may render the appliance inoperable until a factory erase has been performed.

Editing a configuration file

Use this procedure to manually edit configuration files within the Web management console. Binary files cannot be selected and do not have an edit icon.

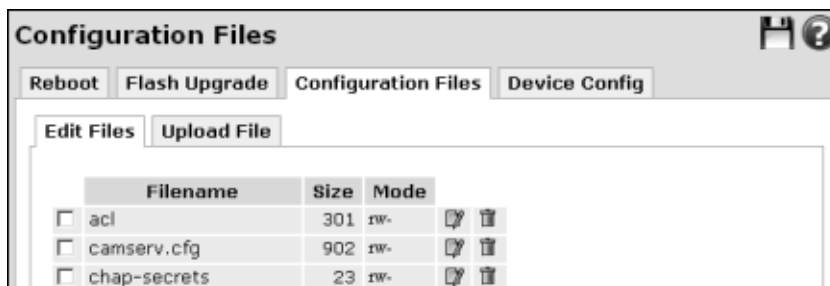


Caution: Make sure you edit in the “Custom entries below here” section if present in the configuration file.

To manually view or edit a configuration file:

- 1 From the **System** menu, click **Advanced > Configuration Files** tab. The Edit File tab appears.

Figure 388:
Edit Files



- 2 To edit a file, select the check box next to the filename and click its edit icon.

Tip: You can also click the **Modify** button at the bottom of the configuration files list. To edit multiple files, select the check boxes for the files and click **Modify**. An edit window opens for each file you want to modify.

The Modify File page appears. The name of the file you are editing displays in the **Filename** field.

Figure 389:
Edit Files

Configuration Files

Reboot Flash Upgrade Configuration Files

Edit Files Upload File

Modify File

Filename

```
root diag=n admin=y sall=n user=n login=y
Buster diag=n admin=n sall=n user=n login=y
Maggie diag=n admin=y sall=n user=n login=n
Gemma diag=y admin=n sall=n user=n login=n
Panda diag=n admin=n sall=n user=n login=n
Harry diag=n admin=n sall=y user=n login=n
Goya diag=n admin=n sall=n user=n login=n
```

Finish Cancel

- 3 Carefully make your edits in the text box.
- 4 Click **Finish**.

Creating a configuration file

Use this procedure to manually create a configuration file from scratch.

- 1 From the **System** menu, click **Advanced > Configuration Files** tab. The Edit File tab appears.
- 2 Scroll to the bottom of the page and click **New**. An empty Modify File page appears.
- 3 Enter the filename, enter the configuration details, and click **Finish**. The file is added to the list of configuration files. Note that any files you create manually have the “x” attribute (able to delete) displayed in the **Mode** column.

Deleting a configuration file

Use this procedure to delete a configuration file. Exercise care when performing this operation as it cannot be reversed.



Caution: Manually deleting the configuration files of your SnapGear appliance may render the appliance inoperable until a factory erase has been performed.

- 1 From the **System** menu, click **Advanced > Configuration Files** tab. The Edit File tab appears.
- 2 Select the delete icon next to the file you want to delete. You are prompted to confirm the delete.
- 3 Click **OK**.

Tip: You can also click the **Delete** button at the bottom of the configuration files list. To delete multiple files, select the check boxes for the files and click **Delete**.

Uploading a configuration file

- 1 From the **System** menu, click **Advanced > Configuration Files > Upload File** tab. The Upload File page appears.

Figure 390:
Upload Configuration
Files

- 2 To locate the file on your local PC that you want to upload, click **Browse**. Locate the file and click Open. Or, type the full path to the file in the **File to Upload** field.
- 3 [Optional] You can upload it to an alternative file name on the SnapGear appliance by specifying another name in the **Destination File Name** field.



Caution: Any existing file with the same name is overwritten.

- 4 Click **Submit**.

Directly viewing or editing the configuration file

Use this procedure to access the page where you can directly view or edit the main configuration file of the appliance.



Caution: Do not edit this file without the assistance of technical support!

- 1 From the **System** menu, click **Advanced > Device Config** tab. The Display/Modify Device Configuration page appears.

Figure 391:
Display/Modify Device
Configuration page



- 2 Make changes only as instructed by technical support personnel.

CHAPTER 6

USB

In this chapter...

USB mass storage devices	524
Example: Partitioning a USB storage device.....	529
USB printers	532
Troubleshooting printing	540
LPR/LPD	542

USB mass storage devices

The SG565 model has two USB (Universal Serial Bus) ports to which you can attach USB devices. USB mass storage devices include USB hard drives, USB flash drives, USB flash card readers loaded with flash cards, and certain digital cameras and portable music players. If you need to attach more than two USB devices simultaneously, you can use a USB hub. You can also attach devices with USB connections such as USB printers and USB narrowband (non-DSL) modems.

Note: *USB DSL modems are not supported at this time.*

Ensure that the USB device is connected using a USB cable if appropriate for the USB device and that the USB device is powered on. Some USB devices, such as USB flash drives, draw their power directly from the USB port; others require a separate power adapter.

USB mass storage devices can be attached to the SnapGear appliance for use as a print spool or to share with your Windows network as a NAS (Network Attached Storage) device. A typical NAS scenario uses the appliance as a network file server.

This chapter includes instructions for configuring your appliance to use the aforementioned USB devices, and for sharing printers and network attached storage on a Windows network.

Once your USB network device or modem has been attached and the appropriate driver loaded, it appears in various configuration pages in the Network Setup menu, such as for Web Cache. For possible configurations, refer to Chapter 2, Network Setup Menu Features.

Sharing a USB storage device

Use this procedure to share a USB storage device.

Note: *USB is applicable to the SG565 model only.*

Prerequisite: Plug a USB storage device into a USB port.

- 1 From the **Network Setup** menu, click **Shares**. The Shares Storage tab appears. Any USB Devices or device Partitions that are available to share are listed along with their Size, and for previously configured shares, their Share Names.

Figure 392: Shares
Storage



- 2 Locate the **USB Device** or device **Partition** you want to share and click its edit icon. An edit page for the USB device appears.

Figure 393: Edit Shares
Storage

Shares

Storage **Printing**

USB Device Flash Disk
Partition 1
Share Name SG565 AV
Description Anti-virus cache
Browsable ☒
Writable ☒
Security Users

User accounts can be created and given share access on the **Local Users** page.

Username
☒ Buster

Finish **Cancel**

- 3 Enter a name for the shared device in the **Share Name** field. This name is displayed when browsing your Windows workgroup.
- 4 [Optional] Enter a description of the device in the **Description** field.
The remaining settings (Browsable, Writable, and Security) control access to the network share from your LAN.
- 5 [Recommended] To display an icon for the network when browsing the network from a Windows PC, select the **Browsable** check box. In order to access the network share when this is not selected, the user must manually enter the address in the address bar (for example, \\SG565\public\).

Tip: For best results, use the IP address of the printer (for example, \\192.168.0.1\public).



Important: The network share must be mapped as a drive within Windows XP in order to allow a username other than the user who is currently logged in. Connect using a different user name before clicking OK when mapping the drive to a letter. If you do not map the drive, the username prompt when logging onto the share is a display-only field indicating the current user for the PC or guest connection.

- 6 [Optional] To make the network share writable, select the **Writable** check box. Users can modify files and create new files.

- 7 Select a security option from the **Security** list. Available options are:
- **Public:** A login and password is not required to access the network share.
 - **Users:** A valid login and password is required to access the network share. Selecting this option displays a list of defined users. Select the check boxes next to the users to whom you want to grant access. For information on adding new users, refer to “Users menu” on page 476.
- 8 Click **Finish**.

Note: If a USB device was configured and removed from the device, “Not Present” is displayed in the **USB Device** column. When you plug the flash drive back into the USB port, the USB Device is detected again after refreshing your browser page.

Figure 394: USB Device
Not Present



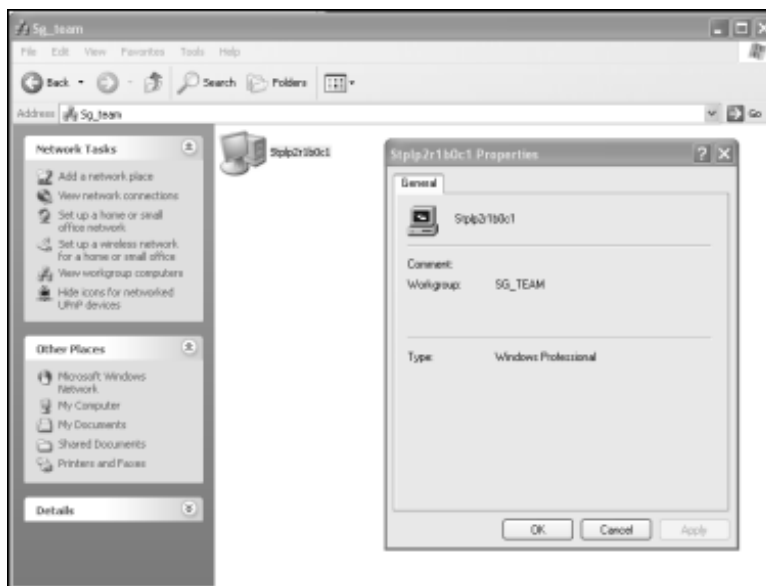
Once configured, you can enable and disable storage shares by selecting and clearing the Enable/Disable check box next to the **Share Name**.

Joining a Windows workgroup

After defining the USB storage share, configure your appliance to join your Windows workgroup. For instructions, see “Entering device settings” on page 151.

Once NAS devices or printers have been shared, your SnapGear appliance becomes visible to other members. To test this, browse from a Windows PC that is a workgroup member. In Windows XP, open **My Network Places** and under **Network Tasks**, click **View workgroup computers** to browse the workgroup.

Figure 395: Windows Workgroup



For information on setting up your Windows workgroup, refer to the documentation shipped with Windows, or the Microsoft Web site.

Example: Partitioning a USB storage device



This example partitions a 128MB USB mass storage device into two equally sized partitions using the SnapGear appliance.

Caution: *This procedure is intended for experts and power users only. Repartitioning a device causes all data on that device to be lost. Back up any data before proceeding. For more details on partitioning, refer to article #3454 in the SnapGear KB: <http://sgkb.securecomputing.com>.*

The appliance supports primary partitions only, so partitions are limited to four. The standard Linux command line tools are present on the SnapGear appliance for partitioning (*fdisk*) and creating filesystems (*mkfs*) on an attached USB mass storage device. Alternatively, you can use the standard Windows tools or a third party utility such as PartitionMagic to partition a USB mass storage device.

- 1 Attach the USB mass storage device.
- 2 After 10 – 15 seconds, from the **System** menu, click **Diagnostics > System Log**. Look for lines similar to the following to see which device name is has been assigned:

```
Apr 22 01:19:49 klogd: USB Mass Storage device found at 4
```

```
Apr 22 01:20:58 klogd: SCSI device sda: 256000 512-byte hdwr  
sectors (131 MB)
```

In this case, the device name is *sda*. If there is a single USB mass storage device attached, it is typically assigned *sda*. If there are multiple USB devices attached, the devices may be *sdb*, *sdc*, and so forth.

- 3 *telnet* or *ssh* to the SnapGear appliance and login. Run the *fdisk* command with the argument */dev/<device name>*:

```
fdisk /dev/sda
```

- 4 Type **p** to display the partition table.

```
Command (m for help): p
```

```
Disk /dev/sda: 5 heads, 50 sectors, 1024 cylinders
```

```
Units = cylinders of 250 * 512 bytes
```

Device	Boot	Start	End	Blocks	Id	System
/dev/sda1		1	1024	127975	b	Win95 FAT32

- 5 Delete any existing partitions by typing **d** then entering the partition number. For example, enter **1** to delete */dev/sda1*.
- 6 Create a new partition by typing **n** then **p** for *primary*, then the partition number.
- 7 Enter the cylinder for the partition to start on. Generally the default is fine.

- 8 Enter the cylinder for the partition to end on, or a size for the partition with *+(size in mb)M*:

```
Command (m for help): n
Command action
    e    extended
    p    primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-1024, default 1):
Using default value 1
Last cylinder or +size or +sizeM or +sizeK (1-1024,
default 1024): +64M
```

- 9 Repeat the process for each partition to want to create. For the last partition, the default last cylinder is generally fine.

```
Command (m for help): n
Command action
    e    extended
    p    primary partition (1-4)
p
Partition number (1-4): 2
First cylinder (526-1024, default 526):
Using default value 526
Last cylinder or +size or +sizeM or +sizeK (526-1024,
default 1024):
Using default value 1024
```

- 10 For each partition, set the partition type to match the type of file system you are going to create on it by typing *t*, the partition number, then the type code (*L* to view type codes). This example creates FAT32 partitions (type code *b*).

```
Command (m for help): t
Partition number (1-4): 1
Hex code (type L to list codes): b
Changed system type of partition 1 to b (Win95 FAT32)
```

- 11 Type *w* to save your changes to the partition table.
- 12 Open the SnapGear management console. From the **System** menu, click **Advanced > Reboot** tab > **Reboot Now**.
- 13 *telnet* or *ssh* to the SnapGear appliance and login.

- 14** For each partition, run the appropriate `mkfs` command. To create FAT32 on our two example partitions:

```
mkfs.vfat -F 32 /dev/sda1
```

then

```
mkfs.vfat -F 32 /dev/sda2
```

- 15** Open the SnapGear management console. From the **System** menu, click **Advanced > Reboot tab > Reboot Now**.

The partitions are now ready to use.

USB printers

The print server of the SnapGear appliance allows you to share attached USB printers with your LAN. After the printer server has been configured, the appliance and printer are displayed when browsing in a Windows workgroup or domain.



Important: Many inexpensive printers do not work with the Print Server for the SnapGear appliance, as their drivers expect the printer to be attached directly to the PC you are printing from, or the printer itself relies on the CPU of the personal computer for processing print jobs (host-based/GDI printers). Due to these technical limitations, SnapGear technical support cannot provide assistance for those types of printers. **It is therefore strongly recommended to use a business-grade printer with the print server.** Non-business grade printers might work, but are unsupported. Additionally, advanced features such as cartridge status reporting might not function correctly. For suggestions, see “Troubleshooting printing” on page 540. Multifunction and all-in-one printers are not supported.

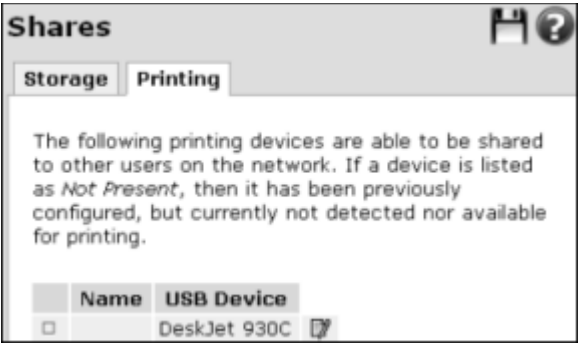
Mac OSX, Linux, and other UNIX-based or UNIX-like machines on the network can use the LPR/LPD protocol for remote printing. For information, see “LPR/LPD” on page 542.

Setting up a shared USB printer

Prerequisite: Attach the USB printer to the SG565 appliance.

- 1 From the **Network Setup** menu, click **Shares > Printing** tab. The Shares Printing page appears. The printer appears in the USB device list but is not enabled since its check box is clear.

Figure 396: Shares
Printing tab



- 2 Locate the printer to share and click its **Edit** icon.

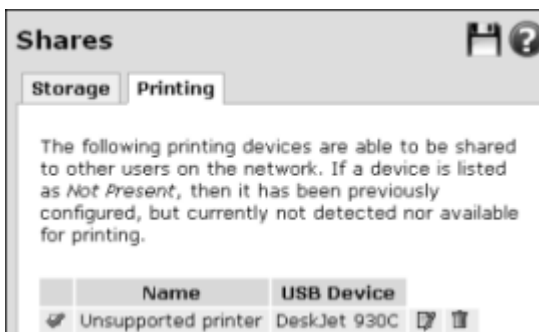
An edit page for the USB printing device appears.

Figure 397: (Edit)
Shares Printing tab



- 3 Enter a short description of the printer in the **Name** field. This name is displayed when browsing your Windows workgroup or domain, and is also the name of the queue for LPR/LPD connections.
- 4 Click **Finish**. A check mark indicates the printer is now enabled in the shared printer list. Make sure you share the device in your domain or workgroup.

Figure 398: Enabled
shared printer



Setting up a printing spool

By default, the SnapGear appliance spools incoming print jobs into memory (RAM) before sending them to a printer. When a Windows PC sends a document or image to the printer attached to the appliance, it first converts it into a format that the printer can read. The resulting file that the appliance has to store in memory can be many times larger than the size of the original document or image. This can be an issue if you have many services running on the appliance (such as many VPN connections, Intrusion Detection, anti-virus, and Web Cache) and the appliance is low on memory, or you intend to print large documents or images.

To avoid the appliance running out of RAM and print jobs failing, it is recommended to use a USB mass storage device for spooling print jobs. You can simultaneously use a USB mass storage device or device partition as a print spool and a Network Attached Storage device; however, the spool directory becomes visible (as spool) and there is a higher chance of the device filling up and causing print jobs to fail. For these reasons, dedicating a partition or device for use as the print spool is recommended.

Prerequisites:

- You must first have connected a printer to the USB port of the appliance and configured the printer. See “Setting up a Windows PC for remote printing” on page 536.
- You must have enabled a USB storage device. See “Sharing a USB storage device” on page 525.

To select a print spool

- 1 From the **Network Setup** menu, click **Shares > Printing** tab. The Shares Printing page appears.

Figure 399: Shares
Printing spool



- 2 Select the device or device partition on which to store the print spool from the **Spool** list.
- 3 Click **Submit**.

Setting up a Windows PC for remote printing

Use this procedure to set up a Windows PC for remote printing. Repeat this procedure for each Windows PC requiring remote printing. This procedure is for the Windows XP Professional operating system. Refer to the Microsoft site for assistance with other flavors of Windows operating systems.

- 1 Click **Start** > **(Settings)** > **Printers and Faxes**. Under **Printer Tasks**, click **Add a printer**.

Figure 400: Windows
Printer Tasks menu



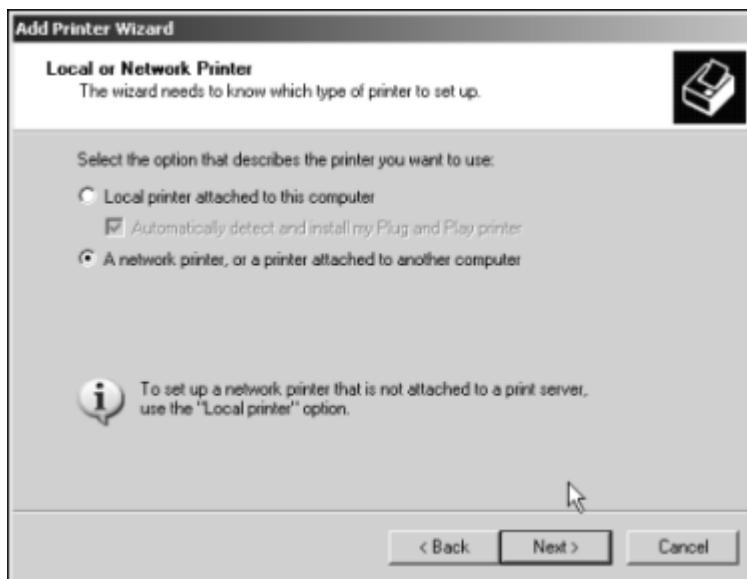
- 2 The **Add Printer Wizard** is displayed.

Figure 401: Windows
Add Printer Wizard -
Welcome



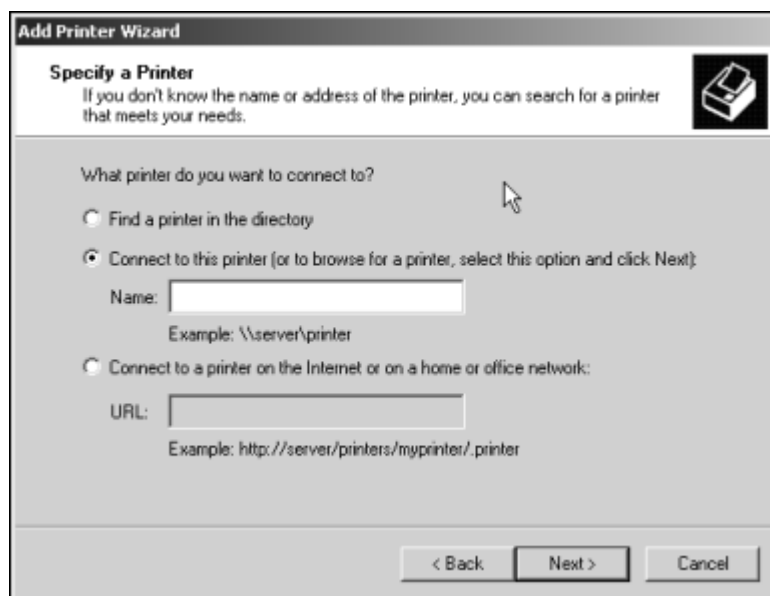
3 Click **Next**.

Figure 402: Windows
Add Printer Wizard - Local
or Network



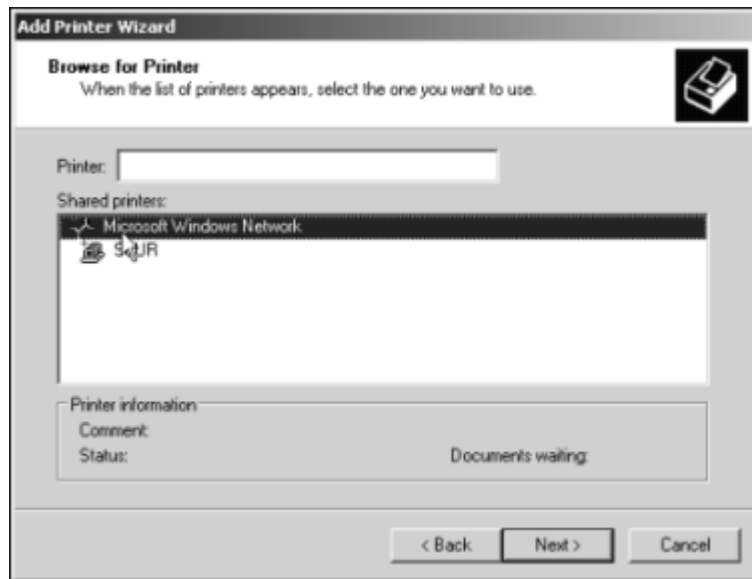
4 Select the **A network printer, or a printer attached to another computer** option and click **Next**. The Specify a Printer page is displayed.

Figure 403: Windows
Add Printer Wizard -
Specify a Printer



5 To browse for a printer, select the **Connect to the printer** option, leave the **Name** blank, and click **Next**. The Browse for a printer page is displayed.

Figure 404: Windows
Add Printer Wizard -
Specify a Printer



- 6 Locate the SnapGear appliance by expanding your Windows workgroup and locating the appliance by its hostname. The hostname is set on the appliance under **Network Setup > System** tab. See “Entering device settings” on page 151. Select the printer and click **Next**.

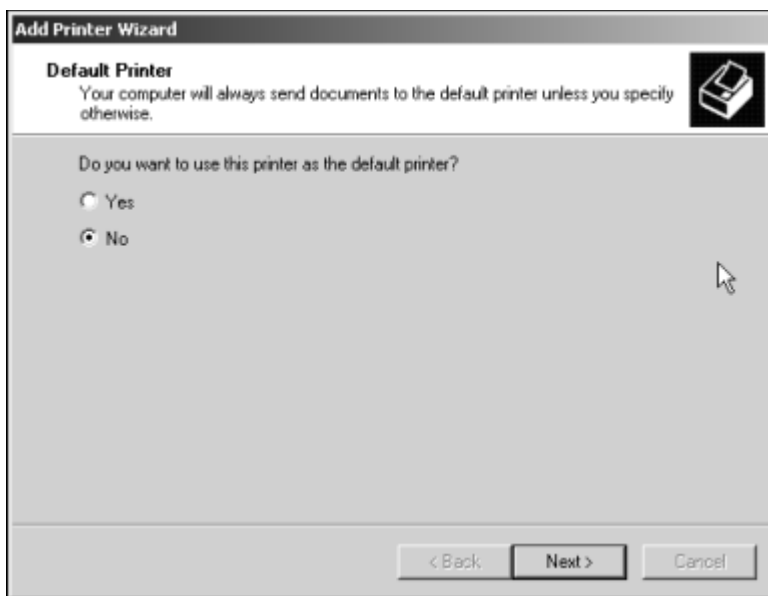
Tip: For best results, use an IP address for the printer name, such as `\\192.168.0.1\printer_share_name`.

- 7 Depending on your printer scenario, follow these instructions:
 - If a warning appears about the appliance automatically installing print drivers on your PC, ignore it; the appliance does not install print drivers automatically.
 - If a message informs you no appropriate print driver could be found, click **OK**. Select the appropriate driver for your printer. If an appropriate printer driver is not already installed on the Windows PC, insert the floppy disk or CD that shipped with your printer, or download the appropriate drivers from the Web site of the manufacturer. You might have to extract this if it is in a compressed archive or .exe format.
 - Click **Have Disk**. Enter the location of the print drivers in **Copy manufacturer's files from** (for example, A: for a floppy or D: for a CD, or the location where you downloaded or extracted the drivers) and click **Browse**.
 - Locate the .inf file for your printer and click **Open** then **OK**. Select your printer model and click **OK**. If your printer model is not listed, click **Have Disk** and **Browse** again. Drivers for several different printers and different operating systems are often distributed together by the manufacturer, so there may be several different .inf files. Follow the onscreen instructions to install the printer driver. This

varies from printer to printer. If you cannot locate the appropriate .inf file or the printer driver fails to install, see “Print driver installation fails” in “Troubleshooting printing” on page 540.

- 8 Choose whether to use this printer as the default printer for this Windows PC and click **Next**.

Figure 405: Windows
Add Printer Wizard -
Default Printer

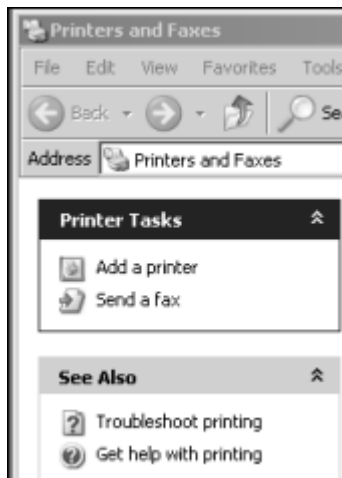


- 9 Click **Finish**.
- 10 To test the printer, print a simple text document from Notepad, or right-click the printer in **Printers and Faxes**, click **Properties > Print Test Page**.

Troubleshooting printing

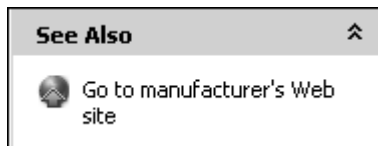
You can troubleshoot printing and access help for printing from within Windows. Under the **Printer Tasks** menu in the **See Also** menu, click **Troubleshoot printing**. This opens printing troubleshooter wizard to assist you. To access online help, click **Get help with printing**. This opens the Resources for troubleshooting printing problems in Windows XP on the Microsoft site.

Figure 406: Windows See Also printing menu



If the printer does appear in the Printer and Faxes area, select the printer so that the printer name appears highlighted. A link appears (under the Printer Tasks menu in the See Also area) for major printer manufacturers, such as HP. Click the **Go to manufacturer's Web site** link to quickly access the site for your printer.

Figure 407: Go to manufacturer's Web site link



This topic contains some common printer issues and steps you can take to resolve them. If none of these address your issue, consult the SnapGear Knowledgebase at:

<http://sgkb.securecomputing.com>

The Knowledgebase also contains information on getting specific printers to interoperate with the SnapGear appliance print server.

Print driver installation fails

- 1 If you are unable to install the remote printer, attach it directly to the Windows PC and follow the manufacturer's instructions to install it as if it were a local printer.
- 2 Once the printer has installed, reconnect it to the SnapGear appliance and follow the instructions in "Setting up a shared USB printer" on page 532. When you are prompted to select the print driver in the Add Printer Wizard, the driver for your printer should now be listed under the manufacturer. If not, visit the Web site of the manufacturer to obtain a printer driver.
- 3 After you complete the wizard, delete the local printer.

Printer appears in *Printers and Faxes*, but printing still fails

Some printers might require you to disable advanced printing features or bidirectional support. Try the following:

Disable advanced printing features

- 1 Click **Control Panel > Printers and Faxes** > right-click *printer name* > **Properties** > **Advanced** tab.
- 2 Clear the **Enable Advanced Printing Features** check box.
- 3 Click **OK**.

Disable bidirectional support

- 1 Click **Control Panel > Printers and Faxes** > right-click *printer name* > **Properties** > **Ports** tab.
- 2 Clear the **Enable bidirectional support** check box.
- 3 Click **OK**.

Printing still fails

Here are a few more troubleshooting suggestions:

- **Print spool memory insufficient:** Check whether you can print a single simple text page from Notepad (**Start** > **Programs** > **Accessories** > **Notepad**). If this works, it is possible your print spool is too small. Enlarge the partition or obtain a USB device with additional memory to dedicate for the print spool.
- **Ensure you are using the correct and most current drivers:** Download the latest drivers from the Web site of the manufacturer.
- **Search the Web:** Search for other user's experiences using your printer model with other print servers. If it does not work with other print servers, it will not work with the SnapGear appliance's print server either. A good resource is online at: http://www.ozcableguy.com/usb_print.html.
- **Enter a support request:** If none of these suggestions are helpful and your printer is business-grade and *not* host-based, enter a support request in the Web ticketing interface on the SnapGear portal. Instructions for the Web ticket system are available online at: <http://sgkb.securecomputing.com>.

LPR/LPD

Note: *The LPR/LPD information is not relevant for Windows network environments.*

Once the print server has been set up, the SnapGear appliance also listens on the standard LPR/LPD network port (TCP 515) for incoming print jobs.

Set up your LPR client to print to a remote LPD queue as specified by the documentation for the operating system. The queue name is the name you specified when setting up the print server.

APPENDIX
A

System Log

In this appendix...

Access logging	544
Creating custom log rules.....	546
Rate limiting.....	548
Administrative access log messages	549
Boot log messages.....	549

Access logging

It is possible to log any traffic that arrives at or traverses the SnapGear appliance. The only logging that is enabled by default is to take note of dropped packets. While it is possible to specifically log exactly which rule led to such a drop, this is not configured by default. All rules in the default security policy drop packets. They never reject them. That is, the packets are simply ignored, and have no responses at all returned to the sender. It is possible to configure reject rules if so desired.

All traffic logging performed on the appliance creates entries in the syslog (/var/log/messages or external syslog server) of the following format:

```
<Date/Time> klogd: <prefix> IN=<incoming interface>  
OUT=<outgoing interface> MAC=<dst/src MAC addresses>  
SRC=<source IP> DST=<destination IP> SPT=<source port>  
DPT=<destination port> <additional packet info>
```

Where:

- <prefix>** if non-empty, hints at cause for log entry
- <incoming interface>** empty, or one of eth0, eth1 or similar
- <outgoing interface>** as per incoming interface
- <dst/src MAC addresses>** MAC addresses associated with the packet
- <source IP>** packet claims it came from this IP address
- <destination IP>** packet claims it should go to this IP address
- <source port>** packet claims it came from this TCP port
- <destination port>** packet wants to go to this TCP port

Depending on the type of packet and logging performed some of the fields may not appear.

Commonly used interfaces are:

- eth0** — the LAN port
- eth1** — the WAN/Internet port
- pppX** — such as *ppp0* or *ppp1*, a PPP session
- IPSecX** — such as *IPSec0*, an IPSec interface

The firewall rules deny all packets arriving from the WAN port by default. There are a few ports open to deal with traffic such as DHCP, VPN services, and similar traffic. Any traffic that does not match the exceptions is dropped.

There are also some specific rules to detect various attacks such as smurf and teardrop. When outbound traffic (from LAN to WAN) is blocked by custom rules configured in the GUI, the resultant dropped packets are also logged.

The *<prefix>* for all these rules is varied according to their type.

Currently used prefixes for arriving traffic:

Default Deny — Packet did not match any rule, drop it

Invalid — Invalid packet format detected

Smurf — Smurf attack detected

Spoof — Invalid IP address detected

SynFlood — SynFlood attack detected

Custom — Custom rule dropped outbound packet

A typical *Default Deny*: looks similar to the following:

```
Mar 27 09:31:19 2003 klogd: Default deny: IN=eth1
OUT=MAC=00:d0:cf:00:ff:01:00:e0:29:65:af:e9:08:00
SRC=140.103.74.181 DST=12.16.16.36 LEN=60 TOS=0x10
PREC=0x00 TTL=64 ID=46341 DF PROTO=TCP SPT=46111 DPT=139
WINDOW=5840 RES=0x00 SYN URGP=0
```

That is, a packet arriving from the WAN (*IN=eth1*) and bound for the appliance itself (*OUT=<nothing>*) from IP address 140.103.74.181 (*SRC=140.103.74.181*), attempting to go to port 139 (*DPT=139*, Windows file sharing) was dropped.

If the packet is traversing the appliance to a server on the private network, the outgoing interface is eth0, as shown in the following example:

```
Mar 27 09:52:59 2003 klogd: IN=eth1 OUT=eth0
SRC=140.103.74.181 DST=10.0.0.2 LEN=60 TOS=0x10
PREC=0x00 TTL=62 ID=51683 DF PROTO=TCP SPT=47044 DPT=22
WINDOW=5840 RES=0x00 SYN URGP=0
```

Packets going from the private network to the public come in eth0, and out eth1, as shown in the following example:

```
Mar 27 10:02:51 2003 klogd: IN=eth0 OUT=eth1 SRC=10.0.0.2
DST=140.103.74.181 LEN=60 TOS=0x00 PREC=0x00 TTL=63
ID=62830 DF PROTO=TCP SPT=46486 DPT=22 WINDOW=5840
RES=0x00 SYN URGP=0
```

Creating custom log rules

Additional log rules can be configured to provide more detail if desired. For example, by analyzing the rules in the Packet Filter Rules menu, it is possible to provide additional log messages with configurable prefixes (that is, other than *Default Deny*;) for some allowed or denied protocols.

Depending on how the *LOG* rules are constructed, it may be possible to differentiate between inbound (from WAN to LAN) and outbound (from LAN to WAN) traffic. Similarly, traffic attempting to access services on the appliance itself can be differentiated from traffic trying to pass through it.

The examples below can be entered on the Command Line Interface (telnet), or into the Packet Filter Rules page in the Web management console. Rules entered on the CLI are not permanent; however, so while it may be useful for some quick testing, it is something to be wary of.

To log permitted inbound access requests to services hosted on the appliance, the rule should look something like this:

```
iptables -I INPUT -j LOG -p tcp --syn -s <X.X.X.X/XX> -d  
<Y.Y.Y.Y/YY> --dport <Z> --log-prefix <prefix>
```

This logs any TCP (*-p tcp*) session initiations (*--syn*) that arrive from the IP address/netmask *X.X.X.X/XX* (*-s ...*) and are going to *Y.Y.Y.Y/YY*, destination port *Z* (*--dport*).

For example, to log all inbound access requests from anywhere on the Internet (0.0.0.0/0) to the PPTP service (port 1723) on the appliance (IP address 1.2.3.4):

```
iptables -I INPUT -j LOG -p tcp --syn -s 0.0.0.0/0 -d  
1.2.3.4 --dport 1723 --log-prefix "Internet PPTP access:  
"
```

To find the resultant log entry in the logs, simply search for the prefix, in this instance *"Internet PPTP access"*.

If, for example, site 192.0.1.2 attempted to access the PPTP port of the appliance, the resultant log message would look something like this:

```
<12> Jan 24 17:19:17 2000 klogd: Internet PPTP access:  
IN=eth0 OUT=  
MAC=00:d0:cf:00:07:03:00:50:bf:20:66:4d:08:00 SRC=  
DST=1.2.3.4 LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=43470 DF  
PROTO=TCP SPT=4508 DPT=1723 WINDOW=64240 RES=0x00 SYN  
URGP=0
```

Notice how *OUT* is set to nothing. This indicates that the packet was attempting to reach a service on the appliance rather than attempting to pass through it.

A very similar scenario occurs for logging access requests that are attempting to pass through the appliance. It merely requires replacing the *INPUT* keyword with *FORWARD*. Thus, to log permitted inbound requests to services hosted on a server behind the appliance, or outbound requests to services on a public network server, use:

```
iptables -I FORWARD -j LOG -p tcp --syn -s <X.X.X.X/XX> -
d <Y.Y.Y.Y/YY> --dport <Z> --log-prefix <prefix>
```

For example, to log all inbound requests from the IP address 5.6.7.8 to the mail server (port 25) on the machine *flubber* on the LAN with address 192.168.1.1:

```
iptables -I FORWARD -j LOG -p tcp --syn -s 5.6.7.8/32 -d
192.168.1.1 --dport 25 --log-prefix "Mail for flubber: "
```

This results in log output similar to:

```
<12> Jan 24 18:17:19 2000 klogd: Mail for flubber:
IN=eth1 OUT=eth0 SRC=5.6.7.8 DST=192.168.1.1 LEN=48
TOS=0x00 PREC=0x00 TTL=126 ID=45507 DF PROTO=TCP SPT=4088
DPT=25 WINDOW=64240 RES=0x00 SYN URGF=0
```

Notice the *OUT* value has now changed to show which interface the access attempt used to reach the internal host. As this request arrived on *eth1* and was destined for *eth0*, it was an *inbound* request, since *eth0* is the LAN port, and *eth1* is usually the WAN port.

An *outbound* request would have *IN=eth0* and *OUT=eth1*.

It is possible to use the *-i* and *-o* arguments to specify the interface that are to be considered for *IN* and *OUT* respectively. When the *!* argument is used before the interface name, the sense is inverted. A name ending in a *+* matches any interface that begins with the name.

```
iptables -I FORWARD -j LOG -i eth0 -p tcp ...
```

This rule logs outbound from the LAN (*eth0*) only. To further limit that, specify which interface it is outbound to, by using the *-o* option:

```
iptables -I FORWARD -j LOG -i eth0 -o eth1 -p tcp ...
```

This logs LAN traffic destined for the WAN, but will not log LAN traffic destined for a PPP or perhaps an IPSec link.

Similarly, you could construct a rule that looks at all inbound/outbound traffic, but excludes VPN traffic, thus:

```
iptables -I FORWARD -j LOG -i eth+ -o eth+ -p tcp ...
```

If you just wanted to look at traffic that went out to the IPsec world, you could use:

```
iptables -I FORWARD -j LOG -o IPsec+
```

There are many more combinations possible. It is possible to write rules that log inbound and outbound traffic, or to construct several rules that differentiate between the two.

Rate limiting

iptables has the facility for rate-limiting the log messages that are generated in order to avoid denial of service issues arising out of logging these access attempts. To achieve this, use the following option:

```
--limit rate
```

rate is the maximum average matching rate, specified as a number with an optional */second*, */minute*, */hour*, or */day* suffix. The default is *3/hour*.

```
--limit-burst number
```

number is the maximum initial number of packets to match. This number gets recharged by one every time the limit specified above is not reached, up to this number. The default is 5.

iptables has many more options. Perform a Web search for *manpage iptables* to find the relevant documentation.

The *LOG* rules configured by default (for example, *Default Deny*;) are all limited to:

```
--limit 3/hour --limit-burst 5
```

Administrative access log messages

When a user tries to log onto the Web management console, one of the following log messages appears:

```
Jan 30 01:54:14 httpd: Authentication successful for root
from 10.46.8.10
Jan 30 23:44:10 httpd: Authentication attempt failed for
root from 10.46.8.1 because: Bad Password
```

The messages show the date and time, whether the authentication succeeded or failed (and reason for the failure), the user attempting authentication (in this case *root*) and the IP address from which the attempt was made.

Successful Telnet (Command Line Interface) login attempts appear as follows:

```
Jan 31 00:06:45 login[32098]: Authentication successful for
root from 10.46.8.66
```

Unsuccessful Telnet login attempts appear as follows:

```
Jan 31 00:09:02 login[32161]: Authentication attempt failed
for root from 10.46.8.66 because: Bad Password
```

The messages show the same information as a Web login attempt.

Successful SSH (Secure Shell) login attempts appear as follows:

```
Jan 31 00:09:14 /bin/sshd[32166]: Accepted password for root
from ::ffff:10.46.8.66 port 1463 ssh2
```

Unsuccessful SSH login attempts appear as follows:

```
Jan 31 00:08:52 /bin/sshd[32154]: Illegal user fred from
::ffff:10.46.8.66
Jan 31 00:08:52 /bin/sshd[32154]: Failed none for illegal
user fred from ::ffff:10.46.8.66 port 1459 ssh2 <6>Jan 31
00:09:14 /bin/sshd[32170]: Address 10.46.8.66 maps to
somepc, but this does not map back to the address - POSSIBLE
BREAKIN ATTEMPT!
```

Boot log messages

The startup boot time messages of the SnapGear appliance are identified by log messages similar to the following:

```
Jan 30 01:54:02 kernel: Linux version 2.4.31-uc0
(build@sbuild) (gcc version 3.3.2) #1 Tue Oct 17 02:00:32
EST 2006
```

This also shows the version of the operating system (Linux), and the build date and time.

APPENDIX
B

Upgrading firmware

In this appendix...

Firmware upgrade best practices and precautions552

Restoring factory default settings553

Upgrading firmware using Netflash553

Recovering from a failed upgrade554

Firmware upgrade best practices and precautions



Caution: If the flash upgrade is interrupted (such as powered down), the SnapGear appliance stops functioning and becomes unusable until its flash is reprogrammed at the factory or a recovery boot is performed. User care is advised.

Prior to performing any firmware upgrade, it is important that you save a back up of your existing configuration to a local file. For more information, see “Backup/Restore menu” on page 469.

Secure Computing makes every effort to ensure an existing configuration, including custom rules and text-file edits, continues to work as intended after upgrading firmware. However, there is no guarantee an entire legacy configuration will transition properly to an upgraded firmware version, particularly in major firmware revision updates. A major firmware revision update, such as from 2.x.y to 3.m.n, often changes underlying subsystems and configuration database formats. When the migration software detects a problem it cannot fix, it reports the details in the firmware upgraded report page. For example, a new version of a subsystem may require an additional configuration parameter that can neither be defaulted nor derived from the existing legacy configuration you wish to restore. In order to maintain a high level of security and assurance that appliance configurations are correct, Secure Computing highly recommends erasing the configuration after a major upgrade and reconfiguring the appliance from scratch. It is extremely unlikely patch and minor releases will ever require factory erasing and reconfiguring.

SnapGear firmware revision numbers have the form *a.b.c*, where *a* is the major revision number, *b* is the minor revision number, and *c* is the patch revision number. An upgrade where the major revision number is incremented is considered a major upgrade; for example, 3.1.5 > 3.2.0. An upgrade where the minor revision number is incremented is considered a minor upgrade, such as 3.0.2 > 3.1.0. An upgrade where the patch revision is incremented is considered a patch upgrade, 3.0.0 > 3.0.1; for example.



Important: Firmware prior to version 3.1.5 did not automatically disable antivirus prior to upgrading, which caused some appliance models to run out of memory. If your installed firmware is version 3.1.4 or earlier, disable antivirus before upgrading.

After the upgrade has completed successfully and the appliance is back up and running with the new firmware, run through a few tests. Ensure that Internet connectivity and any VPN connections can be established and pass traffic, and that any configured services such as DHCP Server, Access Control or Packet Filtering are functioning as expected. If you encounter any problems, reset the device to its factory default settings and reconfigure. You can use a backed up configuration (.sgc) as a guide in this process, but do *not* restore it directly. If you are upgrading a device that you do not normally have physical access to, such as at a remote or client site, it is strongly recommended that following the upgrade, you reset the device to its factory default configuration and reconfigure as a matter of course.

Restoring factory default settings

To restore factory default settings, press the erase button on the rear panel twice within 3 seconds, 1 second apart.

You can also use the SnapGear Web management console to erase the settings for the current configuration and restore the default configuration settings. See “Erasing configuration and rebooting” on page 512.

Upgrading firmware using Netflash

Use this procedure to upgrade your firmware using the Windows *Netflash.exe* utility if your appliance is running a firmware version prior to 2.1.0. Once the appliance is upgraded to version 2.1.0 or higher, you can use the Web management console to upgrade firmware directly using HTTP. The fastest and easiest method of upgrading is using HTTP. For more information, see “Upgrading flash firmware via HTTP” on page 514.

Netflash.exe is a Windows program that automates the upgrade procedure. Be sure to read the onscreen release notes before you attempt the upgrade.

From versions 3.1.0 of the firmware onward, a Netflash upgrade requires two files: the netflash executable and the firmware image (.sgu) appropriate for your appliance. Prior to 3.1.0, the .sgu was bundled into the Netflash Windows executable, which required a separate *Netflash.exe* for each appliance. Once you have downloaded the current *Netflash.exe* file, there will rarely be a need to obtain an updated Netflash executable. Post 3.1.0 firmware does not modify the *Netflash.exe* utility with every firmware release. The files are available in the *images* directory of the SnapGear CD that shipped with your appliance, or can be downloaded from the SnapGear portal at the following URL:

<http://www.securecomputing.com/index.cfm?skey=1597>

Note: *This procedure is not for unresponsive appliances (no Heartbeat or H/B light). Refer to the recovery procedure if that is the case. See “Recovery using Netflash” on page 554.*

- 1 Attach the SnapGear appliance’s LAN port or switch directly to your PC using a straight cable.
- 2 Login to your PC with administrator privileges (2000/XP/NT4 only).
- 3 Ensure there are no DHCP server programs or services (**Start > Run > Open:** *services.msc*) running on your PC.
- 4 Disable the built-in Windows firewall (**Control Panel > Windows Firewall > Off**), and any third party firewall or antivirus software.
- 5 Double-click the Netflash icon to launch it.
- 6 Click **Start Upgrade**. Follow the prompts to complete the upgrade. When prompted, select the appropriate firmware image file (.sgu).

- 7 If you experience any difficulty with the upgrade, refer to the topic “Upgrade using the Windows netflash.exe method” in KB article **#2725**. The URL to the SnapGear portal and knowledgebase is:

<http://sgkb.securecomputing.com>

Recovering from a failed upgrade

Note: Read this topic before requesting an RMA from technical support.

If the Heartbeat (or H/B) LED is not flashing 20–30 seconds after power is supplied, the appliance is unable to boot correctly. This is usually because the firmware inside the appliance has been written incorrectly or incompletely, or in rare cases it may have become corrupt.

In this situation, a recovery boot reprograms the appliance to bring it back to a usable state. This can be done either using Netflash (netflash.exe) if you are running Windows; otherwise, you have to set up a BOOTP (DHCP) server. Both procedures are outlined below.

- “Recovery using Netflash” on page 554
- “Recovery using a BOOTP server” on page 556

Recovery using Netflash

The netflash executable is located in the `\tools` directory on the SnapGear CD, or it can be downloaded from the SnapGear portal. This is a Windows program that automates the recovery procedure. Be sure to read the release notes before attempting the recovery.

To recover your SnapGear appliance using *netflash.exe*, two files are required: The recovery image (*.sgr*) used to recover the appliance, and the firmware image (*.sgu*) appropriate for your appliance. They are available in the *images* directory of the SnapGear CD that shipped with your appliance, or can be downloaded from the SnapGear portal at the following URL:

<http://www.securecomputing.com/index.cfm?skey=1597>

To recover with Netflash

Use the following procedure to perform a recovery boot using the Netflash program on a Windows PC:

- 1 Attach the SnapGear appliance's LAN port or switch directly to your PC using a straight cable.
- 2 Login to your PC with administrator privileges (2000/XP/NT4 only).
- 3 Ensure there are no DHCP server programs or services (**Start > Run > Open:** *services.msc*) running on your PC.

- 4 Disable the built-in Windows firewall (**Control Panel > Windows Firewall > Off**), and any third party firewall or antivirus software.
- 5 Power off the appliance. Press and hold the erase button while powering the appliance on again; keep the erase button held in for 5-10 seconds.
- 6 Double-click the Netflash icon to launch it.
- 7 Click **Recover > Network Recovery**.
- 8 Click **Start Recovery**.
- 9 Enter a free IP address in the same network range as your PC.
- 10 When prompted, select the appropriate recovery image file (.sgr) for your model.
- 11 If the recovery procedure fails at or after the Assigning IP address step, but the Heart Beat/H/B light is flashing, the appliance may have become unreachable due to bad configuration. If this is the case, hit the erase button twice within 3 seconds, 1 second apart to restore factory default configuration, power off the appliance, and restart the recovery procedure from the beginning.
- 12 When prompted, select the appropriate final firmware image file (.sgu). Each .sgu filename designates the model for which it is intended.
- 13 You may be prompted to enter further information, such as your SnapGear appliance's Web administration port or password.
- 14 Wait for the recovery procedure to complete and the appliance to finish reprogramming. It may take up to 15 minutes for your appliance to finish reprogramming. After it has finished, it reboots automatically with its old configuration intact. If it is unreachable after rebooting, press the erase button twice within 3 seconds to restore factory default configuration, then follow the instructions in the *Quick Install Guide* to begin reconfiguration of your appliance.

Recovery using a BOOTP server

To recover your SnapGear appliance using a BOOTP server, two files are required. These are the recovery image (*.sgr*) and final firmware image (*.sgu*) appropriate for your appliance. The image files are available in the *\images* directory of the SnapGear CD that shipped with your appliance.

The following is a brief guide to performing a recovery boot when you are unable to access either Netflash or a Windows PC on which to run it. More comprehensive instructions are not given, as they vary depending on your operating system and server software packages.

The recovery procedure involves network booting the appliance using a BOOTP server with a recovery image file (*.sgr*), then upgrading with a final firmware image file (*.sgu*) as per a normal HTTP or TFTP flash upgrade to reprogram its flash to a usable state.

To perform the recovery boot, you must have a firmware image for your appliance. The firmware that shipped with your appliance is located in the *\firmware* directory on the SnapGear CD. The latest firmware for your appliance can be obtained from the SnapGear portal:

<http://www.securecomputing.com/index.cfm?skey=1597>

Firmware files have the format *Model_Version_Date.sgu* or *Model_Version_Date_*.sgu*.

- 1 Login to your PC with sufficient permissions to edit the server configuration files, and stop and start the servers.
- 2 Place the recovery file (*.sgr*) in the BOOTP server's path and rename it *image.bin*. On Linux operating systems, the path is usually */tftpboot*. Verify the path in your tftp configuration file or the tftpd server documentation. For example:

/tftpboot/image.bin

Note: Due to a bug in the bootloader in some of the SnapGear appliance models (SG560, SG565, SG580), the BOOTP filename argument may not work. You can try using the regular filename of the recovery file. If it does not work, rename the *.sgr* file to "image.bin" as directed in step 2.

- 3 [TFTP upgrades only] If you intend to use the TFTP utility to flash the *.sgu* onto the appliance, place the *.sgu* file into the BOOTP directory as well as the *.sgr* file.

Tip: It is easier to use the HTTP flash upgrade in the Web management console. See "Upgrading flash firmware via HTTP" on page 514.

- 4 Edit your BOOTP server configuration to contain an entry for the appliance. Specify the recovery image file (.sgr) as the file to boot. The entry may look something like the following:

```
host SG300 {  
    hardware ethernet 00:D0:CF:01:02:03;  
    filename "SG300-Recover_v1.0.2_20060224.sgr";  
    fixed-address 192.168.0.100;  
}
```

- 5 Restart the BOOTP server.
- 6 Attach the SnapGear appliance's LAN port or first port of the SnapGear appliance's switch directly to your PC using a straight cable.
- 7 Power off the appliance. Press and hold the erase button while powering the appliance on again; keep the erase button held in for 5-10 seconds.
- 8 After 20–30 seconds, the appliance loads the file from the DHCP/BOOTP server and the H/B light begins flashing.
- 9 Browse or telnet/ssh to your appliance and perform a flash upgrade as per usual to reprogram its flash using the final firmware image (.sgu).

Note: *If the appliance is unreachable, but the Heart Beat/H/B light is flashing, it may be due to bad configuration. If this is the case, press the erase button twice within 3 seconds, 1 second apart to restore the factory default configuration. Perform the network boot again.*

APPENDIX
C

Null modem
administration

In this appendix...

Null modem560

Troubleshooting.....561

Null modem

This appendix details how to enable your SnapGear appliance for administration from a local PC using a null modem serial cable. This allows the local PC to dial in directly to the serial port of the appliance without using a modem. Once the PC is connected, the connection is effectively the same as a remote dial-in connection.

Enabling null modem dial-in

Configure dial-in on the SnapGear appliance as you would for a regular remote dial-in connection, including adding a user name and password if so desired. This is described in detail in “Setting up dial-in access” on page 66.

- 1 From the **System** menu, click **Advanced > Configuration Files** tab.
- 2 Select the edit check box for the *options.ttyS0* file and click **Modify**.
- 3 Remove the following line:

```
connect '/bin/chat -f /etc/config/chat.ttyS0'
```
- 4 Add the following line to the bottom of the file:

```
passive
```
- 5 Click **Finish**.
- 6 Connect the serial port of the appliance directly to the serial port on the local PC using a null modem serial cable. Now follow the procedure, Enabling null modem dial out of the local PC.

Enabling null modem dial out of the local PC

The following instructions are for Windows XP:

- 1 Click **Start > Settings > Control Panel > Network Connections** and select **Create new connection** from the **Network Tasks** menu on the left hand side. Click **Next**.
- 2 Click **Set up an advanced connection** and click **Next**.
- 3 Click **Connect directly to another computer** and click **Next**.
- 4 Click **Guest** and click **Next**.
- 5 In **Computer Name**, enter an arbitrary name for this connection (for example, *SG null modem*) and click **Next**.
- 6 From the **Select device** list, select the local PC's serial (COM) port to which the null modem is attached, and click **Next**.
- 7 Click **Finish**. The network connection now appears under **Network Connections** in **Control Panel** under the **Direct** heading.
- 8 Double-click the connection, enter a dial-in user name and password if you added one on the appliance, and click **Connect**.

Troubleshooting

If you are unable to establish a connection, ensure the serial port settings on the appliance match those of the local PC.

On the SnapGear appliance:

- 1 From the **Network Setup** menu, click Network Setup. The Connections page appears.
- 2 Click the edit icon for the dial-in connection.
- 3 Select the **Port Settings** tab to modify port settings. For details, see “Configuring dialout port settings” on page 61.

If the local PC is running Windows XP, right-click the connection you added in the previous procedure (“Enabling null modem dial out of the local PC” on page 560), select **Properties**, select the **General** tab and click **Configure** to modify port settings.

In this appendix...

Programs and commands	564
-----------------------------	-----

Programs and commands

This appendix contains an alphabetical list of command, programs, and utilities available on each of the SnapGear models for use with the CLI (Command Line Interface). This information is provided as a courtesy in the event you need a function not provided in the Web GUI (SnapGear Management Console), and is intended for expert users. These commands and programs are not supported by Secure Computing technical support. Information about these commands can be obtained by researching them on the Internet.

The following table provides a list of the commands, a short description of the command, and a list of the supported models on which the command is supported.

Table 24: Supported CLI programs and commands

Program Name	Description	Supported Products
arp	Manipulate the system ARP cache	SG560, SG565, SG580, SG640, SG720
auth-down	SnapGear program to run when pptp/ pptpd are brought up	SG300, SG560, SG565, SG580, SG640, SG720
auth-up	SnapGear program to run when pptp/ pptpd are brought down	SG300, SG560, SG565, SG580, SG640, SG720
authd	SnapGear Web and internet access authentication daemon	SG300, SG560, SG565, SG580, SG640, SG720
avscan	Clam anti-virus stand-alone scanner	SG565, SG580, SG640, SG720
awk	Pattern scanning and processing language	SG565, SG580, SG640, SG720
bash	GNU Bourne-Again SHell	SG565, SG580, SG640, SG720
bgpd	BGPv4, BGPv4+, BGPv4- routing engine for use with Zebra	SG560, SG565, SG580, SG640, SG720
bpalogin	Cable login client for BigPond Australia	SG300, SG560, SG565, SG580, SG640, SG720
br	SnapGear bridge control program	SG300, SG560, SG565, SG580, SG640, SG720
brctl	Ethernet bridge administration	SG300, SG560, SG565, SG580, SG640, SG720
busybox	Multi-call UNIX utility binary	SG300, SG560, SG565, SG580, SG640, SG720
camserv	Web cam daemon	SG565
cat	Concatenate files and print on the standard output	SG565, SG580, SG640, SG720

Program Name	Description	Supported Products
chat	Automated conversational script with a modem	SG300, SG560, SG565, SG580, SG720
chgrp	Change group ownership	SG565, SG580, SG640, SG720
chmod	Change file access permissions	SG565, SG580, SG640, SG720
chown	Change file owner and group	SG565, SG580, SG640, SG720
clamboot	SnapGear setup and wrapper program for ClamAV	SG565, SG580, SG640, SG720
clamd	Clam anti-virus daemon	SG565, SG580, SG640, SG720
clamsmtpd	SMTP server for scanning viruses via clamd	SG565, SG580, SG640, SG720
cp	Copy files and directories	SG565, SG580, SG640, SG720
cpio	Copy files to and from archives	SG565, SG580, SG640, SG720
cpu	Simple CPU usage reporting tool	SG565, SG580, SG640, SG720
create-siproxd-conf.tcl	SnapGear tool to create a config file for SIP Proxy	SG560, SG565, SG580, SG640, SG720
cron	Daemon to execute scheduled commands	SG565, SG580, SG640, SG720
date	Print or set the system date and time	SG300, SG560, SG565, SG580, SG640, SG720
dd	Convert and copy a file	SG565, SG580, SG640, SG720
df	Report filesystem disk space usage	SG565, SG580, SG640, SG720
dhcpcd	DHCP client daemon	SG300, SG560, SG565, SG580, SG640, SG720
dhcpcd	Dynamic Host Configuration Protocol Server	SG300, SG560, SG565, SG580, SG640, SG720
dhcrelay	Dynamic Host Configuration Protocol Relay Agent	SG300, SG560, SG565, SG580, SG720
diald	Demand dialing daemon for IP links over phone lines	SG300, SG560, SG565, SG580, SG640, SG720
discard	Network utility that listens on the discard port	SG300, SG560, SG565, SG580, SG640, SG720
dmesg	Print or control the kernel ring buffer	SG565, SG580, SG640, SG720

Program Name	Description	Supported Products
dnsmasq	Caching DNS forwarder	SG300, SG560, SG565, SG580, SG640, SG720
doc_loadbios	Load the BIOS portion of a Disk On Chip	SG720
doc_loadipl	Load an IPL into a DoC Millennium Plus	SG720
dosfsck	Check and repair MS-DOS file systems	SG565
e2fsck	Check a Linux ext2/ext3 file system	SG565, SG720
egrep	Print lines matching a pattern	SG565, SG580, SG640, SG720
enroll	SnapGear CommandCenter program to enroll in a certificate given a CA certificate	SG300, SG560, SG565, SG580, SG640, SG720
erase	Tool for erasing MTD partitions	SG720
eraseall	Tool for erasing entire MTD partitions	SG720
eroute	Manipulate IPSEC extended routing tables	SG300, SG560, SG565, SG580, SG640, SG720
etherwake	Tool to send a Wake-On-LAN Magic Packet	SG300, SG560, SG565, SG580, SG640, SG720
ethtool	Display or change ethernet card settings	SG720
expand	Expand a file with holes into another	SG300, SG560, SG565, SG580, SG640
ez-ipupdate	Utility for updating dynamic DNS host name	SG300, SG560, SG565, SG580, SG640, SG720
false	Do nothing, unsuccessfully	SG300, SG560, SG565, SG580, SG640, SG720
fdisk	Partition table manipulator for Linux	SG565, SG720
firewall	SnapGear firewall utility	SG300, SG560, SG565, SG580, SG640, SG720
firewallenv	SnapGear firewall utility	SG300, SG560, SG565, SG580, SG640, SG720
flash	SnapGear flash utility wrapper	SG300,, SG560, SG565, SG580, SG640, SG720
flashw	Write data to individual flash devices	SG300, SG560, SG565, SG580, SG640, SG720

Program Name	Description	Supported Products
flatfsd	Daemon to save RAM filesystems back to FLASH	SG300, SG560, SG565, SG580, SG640, SG720
freeramdisk	Frees all memory used by the specified ramdisk	SG565, SG580, SG640, SG720
freshclam	Program to download latest ClamAV from the internet	SG565, SG580, SG640, SG720
frox	Transparent ftp proxy and cache	SG565, SG580, SG640, SG720
fsck	Check and repair a Linux file system	SG565, SG720
fsck.ext2	Check a Linux ext2/ext3 file system	SG565, SG720
fsck.msdos	Check and repair MS-DOS file systems	SG565
fsck.vfat	Check and repair MS-DOS file systems	SG565
ftp	Internet file transfer program	SG565, SG580, SG640, SG720
gcc_get_config	SnapGear utility to output config in CommandCenter format	SG300, SG560, SG565, SG580, SG640, SG720
gen-keys	SSH key generation program	SG560, SG565, SG580, SG640, SG720
gen-ssl-cert	SnapGear openssl wrapper	SG300, SG560, SG565, SG580, SG640, SG720
gettyd	Getty daemon	SG300, SG560, SG565, SG580, SG720
gratuitous_arp	SnapGear ARP utility	SG300, SG560, SG565, SG580, SG720
gre	SnapGear GRE Bridging utility	SG300, SG560, SG565, SG580, SG640, SG720
grep	Print lines matching a pattern	SG565, SG580, SG640, SG720
gunzip	Compress or expand files	SG565, SG580, SG640, SG720
gzip	Compress or expand files	SG565, SG580, SG640, SG720
hd	ASCII, decimal, hexadecimal, octal dump	SG565, SG580, SG640, SG720
highavaild	SnapGear High Availability utility	SG300, SG560, SG565, SG580, SG720
hostname	Show or set the system's host name	SG565, SG580, SG640, SG720
htc	HTTP tunnel client	SG560, SG565, SG580, SG640, SG720
hts	HTTP tunnel server	SG560, SG565, SG580, SG640, SG720

Program Name	Description	Supported Products
httpd	FNORD HTTP Web server daemon	SG300, SG560, SG565, SG580, SG640, SG720
https-certgen	SnapGear tool to generate default HTTP SSL certificates	SG300, SG560, SG565, SG580, SG640, SG720
hwclock	Query and set the hardware clock (RTC)	SG560, SG565, SG580, SG720
idb	SnapGear Intrusion Detection & Blocking program	SG300, SG560, SG565, SG580, SG640, SG720
ifconfig	Configure a network interface	SG300, SG560, SG565, SG580, SG640, SG720
ifhasip	SnapGear interface monitoring utility	SG300, SG560, SG565, SG580, SG640, SG720
ifmond	SnapGear interface monitoring daemon	SG300, SG560, SG565, SG580, SG640, SG720
ifready	SnapGear interface monitoring utility	SG300, SG560, SG565, SG580, SG640, SG720
ifretry	SnapGear interface monitoring utility	SG300, SG560, SG565, SG580, SG640, SG720
inetd	Network super-server daemon	SG300, SG560, SG565, SG580, SG640, SG720
inetd-echo	Network echo utility	SG300, SG560, SG565, SG580, SG640, SG720
init	Process control initialization	SG300, SG560, SG565, SG580, SG640, SG720
initconf	SnapGear config initialization utility	SG300, SG560, SG565, SG580, SG640, SG720
insmod	Simple program to insert a module into the Linux Kernel	SG300, SG560, SG565, SG580, SG640, SG720
ip	Show or manipulate routing, devices, policy routing and tunnels	SG300, SG560, SG565, SG580, SG640, SG720
ip6tables	IPv6 packet filter administration	SG560, SG565, SG580, SG640, SG720
ipsec	SnapGear IPSec management utility	SG300, SG560, SG565, SG580, SG640, SG720
ipsecctl	SnapGear IPSec helper utility	SG300, SG560, SG565, SG580, SG640, SG720

Program Name	Description	Supported Products
iptables	Administration tool for IPv4 packet filtering and NAT	SG300, SG560, SG565, SG580, SG640, SG720
iptables-restore	Restore IP Tables	SG300, SG560, SG565, SG580, SG640, SG720
iptables-save	Save IP Tables	SG300, SG560, SG565, SG580, SG640, SG720
iwconfig	Configure a wireless network interface	SG565
iwgetid	Report ESSID, NWID or AP/Cell Address of wireless network	SG565
iwlist	Get more detailed wireless information from a wireless interface	SG565
iwpriv	Configure optionals (private) parameters of a wireless network interface	SG565
kill	Send a signal to a process (SIGTERM by default to end a process gracefully)	SG565, SG580, SG640, SG720
klipsdebug	List or set KLIPS (Kernel IPSEC Support) debug features and level	SG300, SG560, SG565, SG580, SG640, SG720
klogd	Kernel Log Daemon	SG300, SG560, SG565, SG580, SG640, SG720
l2tpd	Layer 2 Tunnelling Protocol Daemon	SG300, SG560, SG565, SG580, SG640, SG720
ln	Make links between files	SG565, SG580,SG640, SG720
logd	SnapGear flash logging utility	SG560, SG565, SG580, SG640, SG720
login	Begin session on the system	SG300, SG560, SG565, SG580, SG640, SG720
lpc	Line printer control program	SG565
lpd	Line printer spooler daemon	SG565
lpq	Spool queue examination program	SG565
lpr	Offline print	SG565
lprm	Remove jobs from the line printer spooling queue	SG565
ls	List directory contents	SG565, SG580, SG640, SG720

Program Name	Description	Supported Products
lsmod	Program to show the status of modules in the Linux Kernel	SG300, SG560, SG565, SG580, SG640, SG720
lspci	List all PCI devices	SG565, SG580, SG640, SG720
mail	Send and receive mail	SG300, SG560, SG565, SG580, SG640, SG720
metash	Noninteractive TCLSH interpreter that loads the metash extensions	SG300, SG560, SG565, SG580, SG640, SG720
mii-tool	View, manipulate media-independent interface status	SG300, SG560, SG565, SG580, SG640, SG720
mkdir	Make directories	SG565, SG580, SG640, SG720
mkdosfs	Create an MS-DOS file system under Linux	SG565
mke2fs	Create an ext2/ext3 file system	SG565, SG720
mkfs.ext2	Check a Linux ext2/ext3 file system	SG565, SG720
mkfs.msdos	Create an MS-DOS file system under Linux	SG565
mkfs.vfat	Create an MS-DOS file system under Linux	SG565
mknod	Make block or character special files	SG565, SG580, SG640, SG720
mkrequest	SnapGear CommandCenter utility to make client certificate request and RSA key	SG300, SG560, SG565, SG580, SG640, SG720
mktemp	Make temporary filename (unique)	SG565, SG580, SG640, SG720
modprobe	Program to add and remove modules from the Linux Kernel	SG565
more	File perusal filter for crt viewing	SG565, SG580, SG640, SG720
mount	Mount a file system	SG565, SG580, SG640, SG720
mount-squid	SnapGear wrapper program to start the squid Web Cache	SG565, SG580, SG640, SG720
mtuchk	SnapGear MTU checking utility	SG300, SG560, SG565, SG580, SG640, SG720
mv	Move (rename) files	SG565, SG580, SG640, SG720
nasl	Nessus Attack Scripting Language	SG565, SG580, SG640, SG720

Program Name	Description	Supported Products
nc	TCP/IP Swiss army knife	SG565, SG580, SG640, SG720
netflash	Upgrade firmware on ucLinux-coldfire platforms using the blkmem interface	SG300, SG560, SG565, SG580, SG640, SG720
netstat	Print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships	SG300, SG560, SG565, SG580, SG640, SG720
nftl_format	Format a Flash Translation Layer	SG720
nftldump	Dump a NAND flash	SG720
nmbd	NetBIOS name server to provide NetBIOS over IP naming services to clients	SG565
ntpd	Network Time Protocol (NTP) daemon	SG300, SG560, SG565, SG580, SG640, SG720
openssl	OpenSSL command line tool	SG300, SG560, SG565, SG580, SG640, SG720
openvpn	Secure IP tunnel daemon	SG565, SG580, SG640, SG720
ospfd	OSPF v2 routing engine for use with Zebra	SG565, SG580, SG640, SG720
passwd	Change user password	SG300, SG560, SG565, SG580, SG640, SG720
pidof	Find the process ID of a running program	SG565, SG580, SG640, SG720
ping	Send ICMP ECHO_REQUEST packets to network hosts	SG300, SG560, SG565, SG580, SG640, SG720
ping6	Send IPv6 pings	SG560, SG565, SG580, SG640, SG720
pluto	IPSec IKE keying daemon	SG300, SG560, SG565, SG580, SG640, SG720
pop3.proxy	POP3 proxy server	SG565, SG580, SG640, SG720
portmap	DARPA port to RPC program number mapper	SG565, SG580, SG640, SG720
pppd	Point-to-Point protocol daemon	SG300, SG560, SG565, SG580, SG640, SG720
pppoe-up	SnapGear program to run when PPPoE connections are brought up	SG300, SG560, SG565, SG580, SG640, SG720

Program Name	Description	Supported Products
pptp	PPTP Client for establishing VPN	SG300, SG560, SG565, SG580, SG640, SG720
pptp_callmgr	PPTP Call manager for the PPTP client	SG300, SG560, SG565, SG580, SG640, SG720
pptpctrl	PPTP VPN controller	SG300, SG560, SG565, SG580, SG640, SG720
pptpd	PPTP VPN daemon	SG300, SG560, SG565, SG580, SG640, SG720
prism2dl	WLAN-NG wireless utility for downloading prism2 images	SG565
proftpd	Professional configurable, secure file transfer protocol server	SG565
proxy80	SnapGear Web proxy daemon	SG300, SG560, SG565, SG580, SG640, SG720
ps	Report a snapshot of the current processes	SG300, SG560, SG565, SG580, SG640, SG720
pwd	Print name of current/working directory	SG565, SG580, SG640, SG720
radauth	Utility to perform authentication against a RADIUS server	SG300, SG560, SG565, SG580, SG640, SG720
radvd	Router advertisement daemon for IPv6	SG560, SG565, SG580, SG640, SG720
radvdump	Dump router advertisements	SG560, SG565, SG580, SG640, SG720
ranbits	Generate random bits in ASCII form	SG300, SG560, SG565, SG580, SG640, SG720
reboot	Safely reboot the system	SG300, SG560, SG565, SG580, SG640, SG720
redialer	SnapGear phone number redialer	SG300, SG560, SG565, SG580, SG720
reports/ activeconn	SnapGear CommandCenter tool to generate reports for active connections	SG300, SG560, SG565, SG580, SG640, SG720
reports/arp	SnapGear CommandCenter tool to generate reports for the ARP table	SG300, SG560, SG565, SG580, SG640, SG720
reports/ diskutil	SnapGear CommandCenter tool to generate reports for Disk Utilization	SG300, SG560, SG565, SG580, SG640, SG720
reports/ interfaces	SnapGear CommandCenter tool to generate reports for Interfaces	SG300, SG560, SG565, SG580, SG640, SG720

Program Name	Description	Supported Products
reports/ intfstats	SnapGear CommandCenter tool to generate reports for Interface Statistics	SG300, SG560, SG565, SG580, SG640, SG720
reports/pfrules	CommandCenter tool to generate reports for Packet Filter Rules	SG300, SG560, SG565, SG580, SG640, SG720
reports/ procstat	SnapGear CommandCenter tool to generate reports for Process List	SG300, SG560, SG565, SG580, SG640, SG720
reports/ protostats	SnapGear CommandCenter tool to generate reports for Protocol Statistics	SG300, SG560, SG565, SG580, SG640, SG720
reports/routes	SnapGear CommandCenter tool to generate reports for Routing Table	SG300, SG560, SG565, SG580, SG640, SG720
reports/ xmlreports.tcl	SnapGear CommandCenter tool to generate reports	SG300, SG560, SG565, SG580, SG640, SG720
ripd	RIP routing engine for use with Zebra	SG560, SG565, SG580, SG640, SG720
rm	Remove files or directories	SG565, SG580, SG640, SG720
rmdir	Remove empty directories	SG565, SG580, SG640, SG720
rmrmmmod	Simple program to remove a module from the Linux Kernel	SG300, SG560, SG565, SG580, SG640, SG720
route	Show or manipulate the IP routing table	SG300, SG560, SG565, SG580, SG640, SG720
route f	IP Route tool to flush IPv4 routes	SG300, SG560, SG565, SG580, SG640, SG720
route l	IP Route tool to list routes	SG300, SG560, SG565, SG580, SG640, SG720
rsasigkey	Generate RSA signature key	SG300, SG560, SG565, SG580, SG640, SG720
rsync	Faster, flexible replacement for rcp	SG565
rt2500apd	Access Point daemon	SG565
rt61apd	802.1x Access Point daemon	SG565
rtacct	Applet printing /proc/net/rt_acct	SG300, SG560, SG565, SG580, SG640, SG720
rtmon	RTnetlink listener	SG300, SG560, SG565, SG580, SG640, SG720
saveall	SnapGear configuration saving utility	SG300, SG560, SG565, SG580, SG640, SG720

Program Name	Description	Supported Products
scp	Secure copy (remote file copy program)	SG560, SG565, SG580, SG640, SG720
sed	Text stream editor	SG565, SG580, SG640, SG720
setmac	Set MAC addresses for eth devices from FLASH	SG560, SG565, SG580, SG640, SG720
setpci	Configure PCI devices	SG565, SG580, SG640, SG720
sgsnmpd	SnapGear CMS SNMP Daemon	SG300, SG560, SG565, SG580, SG640, SG720
sh	Shell	SG300, SG560, SG565, SG580, SG640, SG720
showconfig	SnapGear utility to show device configuration	SG300, SG560, SG565, SG580, SG640, SG720
shtcl	SnapGear TCL shell (interactive)	SG300, SG560, SG565, SG580, SG640, SG720
siproxd	SIP Proxy Daemon	SG560, SG565, SG580, SG640, SG720
sleep	Delay for a specified amount of time	SG565, SG580, SG640, SG720
smbd	Server to provide SMB/CIFS services to clients	SG565
smbmnt	Helper utility for mounting SMB file systems	SG565, SG580, SG640, SG720
smbmount	Mount an SMBFS file system	SG565, SG580, SG640, SG720
smbpasswd	Change a user's SMB password	SG565
smbumount	SMBFS umount for normal users	SG565, SG580, SG640, SG720
smgrd	SnapGear CommandCenter connector daemon	SG300, SG560, SG565, SG580, SG640, SG720
snmpd	SNMP Daemon	SG560, SG565, SG580, SG640, SG720
snort	Open source network intrusion detection system	SG565, SG580, SG640, SG720
snort-inline	SnapGear Snort starter program	SG565, SG580, SG640, SG720
snort-starter	SnapGear Snort starter program	SG565, SG580, SG640, SG720
spi	Manage IPSEC Security Associations	SG300, SG560, SG565, SG580, SG640, SG720

Program Name	Description	Supported Products
spigrp	Group or ungroup IPSEC Security Associations	SG300, SG560, SG565, SG580, SG640, SG720
squid	Web proxy caching server	SG565, SG580, SG640, SG720
squidclient	Command line URL extractor that talks to squid	SG565, SG580, SG640, SG720
sscep	SnapGear CommandCenter SCEP Enrollment utility	SG300, SG560, SG565, SG580, SG640, SG720
ssh	OpenSSH SSH client (remote login program)	SG560, SG565, SG580, SG640, SG720
ssh-keygen	Authentication key generation, management, and conversion	SG560, SG565, SG580, SG640, SG720
sshd	OpenSSH SSH daemon	SG560, SG565, SG580, SG640, SG720
sslwrap	Program that allows plain services to be accessed via SSL	SG300, SG560, SG565, SG580, SG640, SG720
stty	Change and print terminal line settings	SG565, SG580, SG640, SG720
stunnel	Universal SSL tunnel	SG560, SG565, SG580, SG640, SG720
swconfig	SnapGear tool for configuring switches	SG560, SG565, SG580
swtest	SnapGear tool for testing the functionality of the switch	SG560, SG565, SG580, SG720
swvlan	SnapGear VLAN configuration tool	SG560, SG565, SG580
sync	Flush file system buffers	SG565, SG580, SG640, SG720
sysctl	Configure kernel parameters at runtime	SG300, SG560, SG565, SG580, SG640, SG720
syslogd	Linux system logging utilities daemon	SG300, SG560, SG565, SG580, SG640, SG720
tar	The GNU version of the tar archiving utility	SG565, SG580, SG640, SG720
tc	Show or manipulate traffic control settings	SG300, SG560, SG565, SG580, SG640, SG720
tcpblast	Tool for estimating network throughput	SG565, SG580, SG640, SG720
tcpdump	Dump traffic on a network	SG300, SG560, SG565, SG580, SG640, SG720
telnetd	Telnet protocol server	SG300, SG560, SG565, SG580, SG640, SG720

Program Name	Description	Supported Products
test-nasl	SnapGear utility to test NASL vulnerabilities	SG565, SG580, SG640, SG720
testvu	SnapGear CommandCenter program to test validation updates	SG300, SG560, SG565, SG580, SG640, SG720
tip	Simple terminal emulator/cu program for connecting to modems and serial devices	SG300, SG560, SG565, SG580, SG640, SG720
tload	Graphic representation of system load average	SG565, SG580, SG640, SG720
tncfg	Associate IPSEC virtual interface with physical interface	SG300, SG560, SG565, SG580, SG640, SG720
touch	Change file timestamps	SG565, SG580, SG640, SG720
tracepath6	Traces a path to a IPv6 network host discovering MTU along the way	SG560, SG565, SG580, SG640, SG720
tracert	Print the route packets take to network host	SG300, SG560, SG565, SG580, SG640, SG720
tracert6	Traces path to a IPv6 network host	SG560, SG565, SG580, SG640, SG720
true	Do nothing, successfully	SG300, SG560, SG565, SG580, SG640, SG720
tune2fs	Adjust tunable file system parameters on ext2/ext3 file systems	SG565, SG720
umount	Unmount file systems	SG565, SG580, SG640, SG720
uname	Print system information	SG565, SG580, SG640, SG720
unlinkd	Squid unlink daemon	SG565, SG580, SG640, SG720
upnpd	Universal Plug and Play Discovery daemon	SG300, SG560, SG565, SG580, SG640, SG720
usb-acm	SnapGear USB modem helper program	SG565
usb-lpr	SnapGear USB printer helper program	SG565
usb-net	SnapGear USB network device helper program	SG565
usb-storage	SnapGear USB mass storage device helper program	SG565
usleep	Delay for a specified amount of time (micro-seconds)	SG565, SG580, SG640, SG720

Program Name	Description	Supported Products
vconfig	VLAN (802.1q) configuration program	SG300, SG560, SG565, SG580, SG640, SG720
vi	Busybox clone of the VI text editor	SG565, SG580, SG640, SG720
vmstat	Report virtual memory statistics	SG565, SG580, SG640, SG720
vpn-down	SnapGear program to run when pptp/pptpd are brought down	SG300, SG560, SG565, SG580, SG640, SG720
vpn-up	SnapGear program to run when pptp/pptpd are brought up	SG300, SG560, SG565, SG580, SG640, SG720
w	Show who is logged on and what they are doing	SG565, SG580, SG640, SG720
watchdog	Daemon to periodically write to watchdog device	SG300, SG560, SG565, SG580, SG640, SG720
whack	Control interface for IPSEC keying daemon	SG300, SG560, SG565, SG580, SG640, SG720
wlan	SnapGear utility for configuring WLAN (Wireless LAN) connections	SG565
wlancfg	WLAN-NG wireless configuration utility	SG565
wlanctl	WLAN-NG wireless control utility	SG565
wland	WLAN-NG wireless access point daemon	SG565
zcat	Identical to gunzip -c	SG565, SG580, SG640, SG720
zebra	Routing manager for use with associated components	SG560, SG565, SG580, SG640, SG720

APPENDIX
E

Downloading antivirus database files

In this appendix...

Downloading antivirus database files579

Downloading and configuring clam database files

Before clam anti-virus can operate, it is necessary to download the relevant database files. For an appliance normally connected to the Internet, this operation is performed automatically on system boot and again at intervals specified in the Anti-virus configuration page (hourly, daily, weekly). If you have an appliance that is *not* connected to the Internet, it is necessary to manually install the database files. To download the database files, it is necessary to have a machine connected to the Internet. Ideally, the `freshclam` utility that comes with clam anti-virus should be used to download the database files to a local machine. If `freshclam` is not available, you can download the database files from the following URLs:

<http://db.local.clamav.net/main.cvd>

<http://db.local.clamav.net/daily.cvd>

Once you download these two files, the appliance requires access to the files. If you are using a remote share or a USB storage device for anti-virus, it suffices to copy these two files to the top level shared folder. If you are not using a share or local USB storage device, the two files must be copied to the `/var/clamav/` directory. This can be done using `ftp` or `wget` from the appliance. If you are not using a share or local USB storage, you will need to reload the database files whenever the appliance reboots. For more information on USB, see “USB mass storage devices” on page 524. For details on network and local storage for antivirus, see “Auxiliary storage for virus scanning” on page 330. Secure Computing recommends you login to the appliance via `telnet` or `ssh` and validate the database files are installed correctly. The example below changes the directory (`cd` command) to the `clamav` directory and lists the files (`ls` command) within:

```
# cd /var/clamav

# ls -l *.cvd

-rw-r--r--    1 clamav   root 442871 Jan  4 10:24 daily.cvd
-rw-r--r--    1 clamav   root 6924820 Jan  4 10:31 main.cvd
```

The `ls` command lists the two clam files `daily.cvd` and `main.cvd`, their sizes, and permissions (`rw` read/write for owner; `r` read-only for group and everyone). The sizes will vary from the examples shown above (442871 and 6924820). You might have to execute the `chown` and `chmod` commands to correctly set ownership and permissions respectively of the two database files:

```
# chown clamav *.cvd

# chmod 644 *.cvd
```

Typing `chmod 644` sets read/write for the owner, and read-only for group and everyone else (6= rw owner, 4=read only group, 4=read only everyone).

GLOSSARY

List acroADSL	Asymmetric Digital Subscriber Line. A technology allowing high-speed data transfer over existing telephone lines. ADSL supports data rates between 1.5 and 9 Mbits/s when receiving data and between 16 and 640 Kbit/s when sending data.
Advanced Encryption Standard (AES)	The Advanced Encryption Standard is a new block cipher standard to replace DES, developed by NIST, the US National Institute of Standards and Technology. AES ciphers use a 128-bit block and 128-, 192-, or 256-bit keys. The larger block size helps resist birthday attacks while the large key size prevents brute force attacks.
Aggressive Mode	This Phase 1 keying mode automatically exchanges encryption and authentication keys and uses less messages in the exchange when compared to Main mode. Aggressive mode is typically used to allow parties that are configured with a dynamic IP address and a preshared secret to connect or if the SnapGear appliance or the remote party is behind a NAT device.
Authentication	Authentication is the technique by which a process verifies that its communication partner is who it is supposed to be and not an imposter. Authentication confirms that data is sent to the intended recipient and assures the recipient that the data originated from the expected sender and has not been altered en route.
Automatic Keying, Internet Key Exchange (IKE)	This type of keying automatically exchanges encryption and authentication keys and replaces them periodically.
Block cipher	A method of encrypting text (to produce ciphertext) in which a cryptographic key and algorithm are applied to a block of data (for example, 64 contiguous bits) at once as a group rather than to one bit at a time. DES, 3DES and AES are all block ciphers.
BOOTP	Bootstrap Protocol. A protocol that allows a network user to automatically receive an IP address and have an operating system boot without user interaction. BOOTP is the basis for the more advanced DHCP.
CA Certificate	A self-signed certification authority (CA) certificate that identifies a CA. It is called a CA certificate because it is the certificate for the root CA.
Certificates	A digitally signed statement that contains information about an entity and the

entity's public key, thus binding these two pieces of information together. A certificate is issued by a trusted organization (or entity) called a Certification Authority (CA) after the CA has verified that the entity is who it says it is.

Certificate Authority

A Certificate Authority is a trusted third party, which certifies public key's to truly belong to their claimed owners. It is a key part of any Public Key Infrastructure, since it allows users to trust that a given public key is the one they wish to use, either to send a private message to its owner or to verify the signature on a message sent by that owner.

Certificate Revocation List

A list of certificates that have been revoked by the CA before they expired. This may be necessary if the private key certificate has been compromised or if the holder of the certificate is to be denied the ability to establish a tunnel to the SnapGear appliance.

Data Encryption Standard (DES)

The Data Encryption Standard is a block cipher with 64-bit blocks and a 56-bit key.

Dead Peer Detection

The method of detecting if the remote party has a stale set of keys and if the tunnel requires rekeying. To interoperate with the SnapGear appliance, it must conform to the draft draft-ietf-IPSec-dpd-00.txt.

DHCP

Dynamic Host Configuration Protocol. A communications protocol that assigns IP addresses to computers when they are connected to the network.

Diffie-Hellman Group or Oakley Group

The groups used as the basis of Diffie-Hellman key exchange in the Oakley protocol, and in IKE.

Diffie-Hellman Key Exchange

A protocol that allows two parties without any initial shared secret to create one in a manner immune to eavesdropping. Once they have done this, they can communicate privately by using that shared secret as a key for a block cipher or as the basis for key exchange.

Distinguished Name

A list of attributes that defines the description of the certificate. These attributes include: country, state, locality, organization, organizational appliance and common name.

DNS

Domain Name System that allocates Internet domain names and translates them into IP addresses. A domain name is a meaningful and easy to remember name for an IP address.

DUN

Dial Up Networking.

Encapsulating Security Payload (ESP)

Encapsulated Security Payload is the IPSec protocol which provides encryption and can also provide authentication service.

Encryption

The technique for converting a readable message (plaintext) into apparently random material (ciphertext) which cannot be read if intercepted. The proper decryption key is required to read the message.

Ethernet

A physical layer protocol based upon IEEE standards.

Extranet	A private network that uses the public Internet to securely share business information and operations with suppliers, vendors, partners, customers, or other businesses. Extranets add external parties to a company's intranet.
Failover	A method for detecting that the main Internet connection (usually a broadband connection) has failed and the SnapGear appliance cannot communicate with the Internet. If this occurs, the appliance automatically moves to a lower speed, secondary Internet connection.
Fall-forward	A method for shutting down the failover connection when the main Internet connection can be re-established.
Firewall	A network gateway device that protects a private network from users on other networks. A firewall is usually installed to allow users on an intranet access to the public Internet without allowing public Internet users access to the intranet.
Gateway	A machine that provides a route (or pathway) to the outside world.
Hashes	A code, calculated based on the contents of a message. This code should have the property that it is extremely difficult to construct a message so that its Hash comes to a specific value. Hashes are useful because they can be attached to a message, and demonstrate that it has not been modified. If a message were to be modified, then its hash would have changed, and would no longer match the original hash value.
Hub	A network device that allows more than one computer to be connected as a LAN, usually using UTP cabling.
IDB	Intruder Detection and Blocking. A feature of your SnapGear appliance that detects connection attempts from intruders and can also optionally block all further connection attempts from the intruder's machine.
Internet	A worldwide system of computer networks. A public, cooperative, and self-sustaining network of networks accessible to hundreds of millions of people worldwide. The Internet is technically distinguished because it uses the TCP/IP set of protocols.
Intranet	A private TCP/IP network within an enterprise.
IP Compression	A good encryption algorithm produces ciphertext that is evenly distributed. This makes it difficult to compress. If one wishes to compress the data it must be done prior to encrypting. The IPcomp header provides for this. One of the problems of tunnel mode is that it adds 20 bytes of IP header, plus 28 bytes of ESP overhead to each packet. This can cause large packets to be fragmented. Compressing the packet first may make it small enough to avoid this fragmentation.
IPSec	Internet Protocol Security. IPSec provides interoperable, high quality, cryptographically-based security at the IP layer and offers protection for network communications.
IPSec tunnel	The IPSec connection to securely link two private parties across insecure and

	public channels.
IPSec with Dynamic DNS	Dynamic DNS can be run on the IPSec endpoints thereby creating an IPSec tunnel using dynamic IP addresses.
IKE	IKE is a profile of ISAKMP that is for use by IPSec. It is often called simply IKE. IKE creates a private, authenticated key management channel. Using that channel, two peers can communicate, arranging for sessions keys to be generated for AH, ESP or IPcomp. The channel is used for the peers to agree on the encryption, authentication and compression algorithms to be used. The traffic to which the policies are applied is also agreed upon.
ISAKMP	ISAKMP is a framework for doing Security Association Key Management. It can, in theory, be used to produce session keys for many different systems, not just IPSec.
Key lifetimes	The length of time before keys are renegotiated.
LAN	Local Area Network.
LED	Light-Emitting Diode.
Local Private Key Certificate & Passphrase	The private part of the public/private key pair of the certificate resides on the SnapGear appliance. The passphrase is a key that can be used to lock and unlock the information in the private key certificate.
Local Public Key Certificate	The public part of the public/private key pair of the certificate resides on the SnapGear appliance and is used to authenticate against the CA certificate.
MAC address	The hardware address of an Ethernet interface. It is a 48-bit number usually written as a series of 6 hexadecimal octets; for example 00:d0:cf:00:5b:da. A SnapGear appliance has a MAC address for each Ethernet interface. These are listed on a label underneath the appliance.
Main Mode	This Phase 1 keying mode automatically exchanges encryption and authentication keys and protects the identities of the parties attempting to establish the tunnel.
Manual Keying	This type of keying requires the encryption and authentication keys to be specified.
Manual Keys	Predetermined encryption and authentication keys used to establish the tunnel.
Masquerade	The process when a gateway on a local network modifies outgoing packets by replacing the source address of the packets with its own IP address. All IP traffic originating from the local network appears to come from the gateway itself and not the machines on the local network.
MD5	Message Digest Algorithm Five is a 128 bit hash. It is one of two message digest algorithms available in IPSec.
NAT	Network Address Translation. The translation of an IP address used on one

	network to an IP address on another network. Masquerading is one particular form of NAT.
Net mask	The way that computers know which part of a TCP/IP address refers to the network, and which part refers to the host range.
NTP	Network Time Protocol (NTP) used to synchronize clock times in a network of computers.
Oakley Group	See Diffie-Hellman Group or Oakley Group.
PAT	Port Address Translation. The translation of a port number used on one network to a port number on another network.
PEM, DER, PKCS#12 PKCS#07	These are all certificate formats.
Perfect Forward Secrecy	A property of systems such as Diffie-Hellman key exchange which use a long-term key (such as the shared secret in IKE) and generate short-term keys as required. If an attacker who acquires the long-term key provably can neither read previous messages which he may have archived nor read future messages without performing additional successful attacks then the system has PFS. The attacker needs the short-term keys in order to read the traffic and merely having the long-term key does not allow him to infer those. Of course, it may allow him to conduct another attack (such as man-in-the-middle) which gives him some short-term keys, but he does not automatically get them just by acquiring the long-term key.
Phase 1	Sets up a secure communications channel to establish the encrypted tunnel in IPSec.
Phase 2	Sets up the encrypted tunnel in IPSec.
PPP	Point-to-Point Protocol. A networking protocol for establishing simple links between two peers.
PPPoE	Point to Point Protocol over Ethernet. A protocol for connecting users on an Ethernet to the Internet using a common broadband medium (for example, single DSL line, wireless device, or cable modem).
PPTP	Point to Point Tunneling Protocol. A protocol developed by Microsoft that is popular for VPN applications. Although not considered as secure as IPSec, PPP is considered "good enough" technology. Microsoft has addressed many flaws in the original implementation.
Preshared secret	A common secret (passphrase) that is shared between the two parties.
Quick Mode	This Phase 2 keying mode automatically exchanges encryption and authentication keys that actually establishes the encrypted tunnel.
Rekeying	The process of renegotiating a new set of keys for encryption and authentication.

Road warrior	A remote machine with no fixed IP address.
Router	A network device that moves packets of data. A router differs from hubs and switches because it is intelligent and can route packets to their final destination.
RSA Digital Signatures	A public/private RSA key pair used for authentication. The SnapGear appliance can generate these key pairs. The public keys need to be exchanged between the two parties in order to configure the tunnel.
SHA	Secure Hash Algorithm, a 160-bit hash. It is one of two message digest algorithms available in IPSec.
Security Parameter Index (SPI)	Security Parameter Index, an index used within IPSec to keep connections distinct. Without the SPI, two connections to the same gateway using the same protocol could not be distinguished.
Subnet mask	See Net mask.
Switch	A network device that is similar to a hub, but much smarter. Although not a full router, a switch particularly understands how to route Internet packets. A switch increases LAN efficiency by utilizing bandwidth more effectively.
TCP/IP	Transmission Control Protocol/Internet Protocol. The basic protocol for Internet communication.
TCP/IP address	Fundamental Internet addressing method that uses the form nnn.nnn.nnn.nnn.
TripleDES (3DES)	Using three DES encryptions on a single data block, with at least two different keys, to get higher security than is available from a single DES pass.
UTC	Coordinated Universal Time.
UTP	Unshielded Twisted Pair cabling. A type of Ethernet cable that can operate up to 100Mbps/s. Also known as Category 5 or CAT 5.
VPN	Virtual Private Networking. When two locations communicate securely and effectively across a public network (such as the Internet). The three key features of VPN technology are privacy (nobody can see what you are communicating), authentication (you know who you are communicating with), and integrity (nobody can tamper with your messages/data).
WAN	Wide Area Network.
WINS	Windows Internet Naming Service that manages the association of workstation names and locations with IP addresses.
x.509 Certificates	An x.509 certificate includes the format of the certificate, the serial number of the certificate, the algorithm used to sign the certificate, the name of the CA that issued the certificate, the name and public key of the entity requesting the certificate, and the CA's signature.x.509 certificates are used to authenticate the remote party against a Certificate Authority's (CA) certificate. The CA

certificate must have signed the local certificates that are used for tunnel authentication. Certificates need to be uploaded into the SnapGear appliance before a tunnel can be configured to use them.

INDEX

Numerics

- 1-to-1 NAT
 - deleting rule 266
 - disabling rule 266
 - enabling rule 266

A

- access control
 - disabling 300
 - enabling 298
- account
 - creating dynamic DNS 156
 - deleting dynamic DNS 159
 - disabling dynamic DNS 159
 - editing dynamic DNS 159
- ACL 110, 304
- adding
 - alias IP address for interface 43
 - CA certificate 432
 - CRL certificate 434
 - local certificate 431
 - local user 480
 - NTP peer 468
 - NTP server 468
 - port-based VLAN 132
 - PPTP user 355
 - VLAN 127
- Addresses
 - IP 223
- administrative
 - deleting user 478
 - editing user 478
- ADSL 46
- advanced
 - wireless configuration 116
- agent
 - disabling SNMP 496
 - enabling SNMP 495

- alias IP address
 - adding for interface 43
 - deleting for interface 44
- aliases
 - interface 43
- allowing
 - URL 307
- antispam 340
- antivirus 327
 - disabling 329
 - enabling 328
 - local USB storage 331
 - network share 330
- appliance
 - halt now 512
- Arp 564
- Authd 564
- auth-down 564
- authenticating
 - tunnels via preshared secret 369
 - tunnels via x509 certificate 368
- auth-up 564
- availability
 - high 86
- Avscan 564
- Awk 564

B

- balancing
 - load 84
- Bash 564
- Baud rate 61
- beacon frames 116
- BGP 149
- Bgpd 564
- blocking
 - categories Webwasher URL 323
 - URL 308
- boot

- log messages 549
- Border Gateway Protocol 149
- bplogin 564
- br (bridge control) program 564
- brcntrl program 564
- bridge
 - deleting 126
- bridged mode 9
- bridging network interfaces 119
- busybox 564

C

- CA
 - adding certificate 432
- CA certificate
 - creating 421
- cable
 - modem 55
- cache
 - disabling Web 178
 - enabling Web 177
 - Web 176, 182
- camserv daemon 564
- capture
 - packet 506
- cat command 564
- certificate
 - adding CA 432
 - adding CRL 434
 - adding local 431
 - creating CA 421
 - creating SSL 211
 - deleting 434
 - extracting PKCS12 420
 - HTTPS 210
 - uploading SSL 210
 - uploading Webwasher 321
- chat 565
- chgrp command 565
- chmod command 565
- chown command 565
- clamboot program 565
- clamd 565
- clamsmtpd server 565
- client
 - configuring HTTP tunnel 453
 - ICAP 186
 - L2TP VPN 373
 - PPTP VPN 349
- CMS
 - Device Attributes 493
 - disabling 492
 - enabling 490
- CMS device attribute
 - deleting 494
 - editing 494
- command
 - cat 564
 - chgrp 565
 - chmod 565
 - chown 565
 - cp 565
 - cpio 565
 - IPSec 568
 - kill 569
 - mount 570
 - pidof 571
 - ping 571
 - snort 574
- CommandCenter
 - debug logging 488
 - disabling debug logging 488
- configuration
 - deleting file 521
 - deleting local file 473
 - erasing and rebooting 512
 - restoring local file 473
 - restoring remote backup 471
- configuration file
 - creating 520
 - direct display 522
 - direct edit 522
 - editing 519
 - uploading 521
- configuring
 - advanced Web Cache settings 187
 - advanced wireless features 116
 - DHCP 164
 - DHCP relay 171
 - DMZ connection 95
 - guest connection 98
 - IDB 285
 - IDS Snort 294
 - local system log 499
 - Web management console 208
 - wireless connection 100
- connecting
 - dial-in Windows XP client 69
- connection

- configuring DMZ 95
- configuring guest 98
- configuring wireless 100
- direct 38
- disabling 36
- disabling IPv6 45
- editing 36
- editing failover parameters 77
- logging 274
- preventing flooding 275
- viewing 36
- connection tracking 274
 - FTP 274
 - H.323 274
 - IRC 274
 - PPTP 274
 - TFTP 274
- console
 - configuring Web management 208
- content filtering
 - disabling Webwasher 321
- cp command 565
- cpio command 565
- creating
 - 1-to-1 NAT rule 264
 - advanced port forwarding rule 250
 - basic port forwarding rule 249
 - CA certificate 421
 - configuration file 520
 - dynamic DNS account 156
 - packet priority rule 194
 - security policy group 313
 - service group 221
 - source NAT rule 258
 - SSL certificate 211
 - static host 160
- CRL
 - adding certificate 434
- custom
 - firewall rule 241
 - iptables 241
- Custom Firewall Rules tab 242
- Custom IPv6 Firewall Rules tab 244

D

- debug logging
 - disabling CommandCenter 488
- defining
 - Interface Group 227

- Definitions menu 219
- deleting
 - 1-to-1 NAT rule 266
 - administrative user 478
 - alias IP address for interface 44
 - blocked URL 308, 310
 - bridge 126
 - certificate 434
 - CMS device attribute 494
 - configuration file 521
 - DHCP server or relay configuration 167
 - dynamic DNS account 159
 - dynamic IP address 170
 - Interface Group 228
 - IPSec VPN tunnel 386
 - L2TP IPSec tunnel 369
 - local configuration file 473
 - local user 482
 - NASL script 316
 - packet capture file 509
 - packet filter rule 236
 - packet priority rule 195
 - port forwarding rule 253
 - port tunnel 460
 - port-based VLAN 135
 - security policy group 314
 - service group 222
 - source NAT rule 262
 - static host 161
- detected devices
 - USB 505
- device
 - serial number 152
- DHCP
 - configuring 164
 - deleting server or relay configuration 167
 - disabling server or relay 166
 - proxy 171
 - re-enabling server or relay 166
 - relay 171
 - server 162
- DHCP Addresses page 167
- DHCP relay
 - configuring 171
- DHCP Status page 163
- dial on demand
 - disabling 64
- dial on demand connection
 - enabling 63
- dial out

- null modem 560
 - dial-in
 - connecting Windows XP client 69
 - null modem 560
 - dialout
 - port settings 61, 65
 - direct
 - connection 38
 - disabling
 - 1-to-1 NAT rule 266
 - access control 300
 - antivirus 329
 - CMS 492
 - CommandCenter debug logging 488
 - connection 36
 - DHCP server or relay 166
 - dial on demand 64
 - DNS proxy server 154
 - dynamic DNS account 159
 - high availability 91
 - IPSec VPN 386
 - IPSec VPN tunnel 386
 - IPv6 197
 - IPv6 for connection 45
 - masquerading 269
 - NASL script 316
 - packet capture file 508
 - packet filter rule 236
 - port forwarding rule 252
 - port tunnel 460
 - QoS Autoshaper 191
 - security policy enforcement 312
 - SIP proxy 199
 - SNMP agent 496
 - source NAT rule 261
 - TrustedSource 345
 - Web cache 178
 - Webwasher content filtering 321
 - DMZ 94
 - configuring connection 95
 - DNS 153
 - creating dynamic account 156
 - deleting dynamic account 159
 - disabling dynamic account 159
 - dynamic 155
 - editing dynamic account 159
 - proxy 154
 - DNS proxy server
 - disabling 154
 - Domain Name System 153

- downloading
 - packet capture file 508
 - dummy services 287, 290
 - dynamic
 - DNS 155
 - dynamic DNS account
 - creating 156
 - deleting 159
 - disabling 159
 - editing 159
 - dynamic IP address
 - deleting 170

E

- editing
 - 1-to-1 NAT rule 265
 - administrative user 478
 - CMS device attribute 494
 - configuration file 519
 - connection 36
 - dynamic DNS account 159
 - failover connection parameters 77
 - Interface group 228
 - local user 482
 - packet filter rule 236
 - packet priority rule 195
 - port forwarding rule 252
 - port tunnel 459
 - port-based VLAN 134
 - service group 222
 - static host 161
- email
 - POP 333, 334
- enabling
 - 1-to-1 NAT rule 266
 - access control 298
 - antivirus 328
 - CMS 490
 - CommandCenter Debug Logging 488
 - dial on demand connection 63
 - FTP antivirus scanning 338
 - high availability 91, 92
 - IPSec 378
 - IPv6 196
 - load balancing 84
 - masquerading 268
 - packet filter rule 236
 - port forwarding rule 253
 - port-based VLAN 130

- QoS Autoshaper 190
- route management 143
- SNMP agent 495
- source NAT rule 262
- Web cache 177
- erasing
 - configuration and rebooting 512
- extended ISO date
 - timestamping 499
- extracting
 - certificate 420

F

- factory default
 - restoring firmware 553
- factory default settings
 - returning to 512
- failover
 - IPSec 435
 - modifying levels 81
- fdisk 529
- file
 - deleting configuration 521
 - deleting packet capture 509
 - disabling packet capture 508
 - downloading packet capture 508
 - editing configuration 519
 - PAC 177
 - uploading configuration 521
- firewall
 - custom rule 241
- firmware
 - flash upgrade HTTP 514
 - flash upgrade TFTP 516
 - restoring factory default settings 553
 - upgrading with Netflash 553
- flash upgrade
 - HTTP 514
 - TFTP 516
- flood rate limiting 275
- flooding
 - preventing connection 275
- fragmentation
 - packet 116
- freeing
 - IP addresses 169
- FTP
 - connection tracking 274
 - enabling antivirus scanning of 338

G

- gateway
 - UPnP 270
- GRE tunnel 136
 - troubleshooting 138
- group
 - security policy enforcement 313
- guest connection
 - configuring 98
- guest network 97

H

- H.323
 - connection tracking 274
 - protocol 276
- halt
 - appliance 512
- hardware
 - serial number 152
- Help
 - online 26
- high availability 86
 - disabling 91
 - enabling 91, 92
- host
 - creating static 160
 - deleting static 161
 - editing static 161
- HTTP
 - flash firmware upgrade 514
 - tunnel client 453
 - tunnel server 455
- HTTPS
 - certificate 210

I

- ICAP
 - client 186
- IDB 285
- IDS Snort
 - configuring 294
- interface
 - aliases 43
- Interface Group
 - defining 227
 - deleting 228

- editing 228
- Interfaces tab 227
- Internet Relay Chat
 - connection tracking 274
- Intrusion Detection and Blocking 285
- IP address
 - adding alias for interface 43
 - deleting alias for interface 44
 - deleting dynamic 170
 - freeing leased 169
 - rebooted SnapGear 513
 - reserving 170
 - static 64
- IPSec
 - disabling VPN 386
 - enabling 378
 - failover 435
 - offloading VPN 444
- IPSec command 568
- IPSec VPN 410
- IPSec VPN tunnel
 - deleting 386
 - disabling 386
- IPSec VPN tunnels
 - refreshing status 382
- iptables 241
- IPv6 44, 196
 - Custom Firewall Rules 244
 - disabling 197
 - disabling for connection 45
 - enabling 196
- IRC 274

K

- kill command 569

L

- L2TP
 - VPN client 373
 - VPN server 363
- L2TP IPSec tunnel
 - deleting 369
- LEDs 3, 10
- limitation
 - port-based VLAN 130
- limitations
 - load balancing 83
- limiting

- rate 548
- load balancing 83
 - enabling 84
 - limitations 83
- local
 - adding certificate 431
 - adding user 480
 - deleting configuration file 473
 - deleting user 482
 - editing user 482
 - restoring configuration file 473
- Local Backup/Restore 472
- local configuration file
 - deleting 473
 - restoring 473
- Local Syslog tab 499
- local system log
 - configuring defaults 499
- local USB storage
 - antivirus 331
- Locality 463
- log
 - boot messages 549
- logging
 - CommandCenter Debug 488
 - connection 274
- LPD 542
- LPR/LPD 542

M

- masquerading
 - disabling 269
 - enabling 268
- menu
 - Definitions 219
- message
 - boot log 549
- mkfs 529
- mode
 - bridged 9
- modem
 - cable 55
- mount command 570

N

- NAS 524
- NASL
 - uploading scripts 316

- NASL script
 - deleting 316
 - disabling 316
- NAT 245
 - creating 1-to-1 rule 264
 - creating source rule 258
 - deleting 1-to-1 rule 266
 - deleting source rule 262
 - disabling 1-to-1 rule 266
 - disabling source rule 261
 - editing 1-to-1 rule 265
 - enabling 1-to-1 rule 266
 - enabling source rule 262
 - source 257
 - traversal support 419
- Netflash
 - recovery 554
 - upgrading firmware 553
- netmask
 - rebooted SnapGear 513
- network
 - guest 97
- Network Address Translation 245
- Network Attached Storage 524
- network port
 - TCP 515 542
- network share
 - antivirus 330
- network storage
 - Web cache 180
- NTP
 - adding peer 468
 - adding server 468
- null modem
 - dial out 560
 - dial-in 560
 - serial cable 560

O

- offloading
 - IPSec VPN 444
- online
 - Help 26
- Open Shortest Path First 146
- OpenSSL 420
- OSPF 146

P

- PAC file 177
- packet
 - capture 506
 - fragmentation 116
- packet capture
 - deleting file 509
 - disabling file 508
 - downloading file 508
- packet filter rule
 - deleting 236
 - disabling 236
 - editing 236
 - enabling 236
- packet priority rule
 - creating 194
 - deleting 195
 - editing 195
- partitioning
 - USB storage device 529
- pcap file
 - deleting 509
 - disabling 508
 - downloading 508
- PCI DSS 479
- peer
 - adding NTP 468
- peers 185
- persistent
 - system log 501
- pidof command 571
- ping command 571
- ping test 503
- PKCS12
 - extracting certificate 420
- PKCS12 format file 423
- policy
 - routes 141
- POP
 - email 333, 334
- port
 - 5060 198
- port forwarding
 - deleting rule 253
 - disabling rule 252
 - editing rule 252
 - enabling rule 253
- Port Forwarding page 248
- port forwarding rule

- creating advanced 250
 - creating basic 249
- port settings
 - dialout 61, 65
- port tunnel
 - deleting 460
 - disabling 460
 - editing 459
- port-based VLAN
 - adding 132
 - deleting 135
 - editing 134
 - limitations 130
- ports
 - multifunction vs. fixed-function 34
- PPTP
 - adding user 355
 - connection tracking 274
 - enabling VPN server 353
 - VPN client 349
 - VPN server 352
- preshared secret
 - authenticating tunnel 369
- preventing
 - connection flooding 275
- print
 - spool 534
- print server 532
- printing
 - remote 536
- program
 - clamboot 565
 - Zebra 577
- protocol
 - border gateway 149
 - H.323 276
 - session initiation 198
 - spanning tree 122
- proxy
 - DHCP 171
 - DNS 154
 - SIP 198
- Proxy Automatic Configuration file. See PAC file

Q

- QoS Autoshaper
 - disabling 191
 - enabling 190

- QoS traffic shaping 190

R

- RADIUS server 483
- rate limiting 237, 548
- reboot
 - soft 511
- recover
 - Netflash 554
- re-enabling
 - DHCP server or relay 166
- refresh
 - view of UPnP port forwards 273
- refreshing
 - VPN IPsec tunnel status 382
- relay
 - configuring DHCP 171
 - DHCP 171
- remote
 - printing 536
 - restoring configuration 471
 - system log 501
- report
 - technical support 28
- reports
 - viewing Webwasher URL filtering 324
- reserving
 - IP address 170
- restoring
 - firmware factory default settings 553
 - local configuration file 473
 - remote configuration backup 471
- RIP 144
- root user 476
- route
 - trace test 504
- route management
 - enabling 143
- routes
 - policy 141
 - static 139
- RTS (Request To Send) 116
- rule
 - creating 1-to-1 NAT 264
 - creating source NAT 258
 - custom firewall 241
 - deleting 1-to-1 NAT 266
 - deleting port forwarding 253
 - deleting source NAT 262

- disabling 1-to-1 NAT 266
- disabling port forwarding 252
- disabling source NAT 261
- editing 1-to-1 NAT 265
- editing port forwarding 252
- enabling 1-to-1 NAT 266
- enabling port forwarding 253
- enabling source NAT 262

S

- scanning
 - FTP for viruses 338
- scripts
 - uploading NASL 316
- security policy enforcement
 - disabling 312
- security policy group
 - creating 313
 - deleting 314
- serial cable
 - null modem 560
- serial number 152
- server
 - adding NTP 468
 - configuring HTTP tunnel 455
 - DHCP 162
 - enabling PPTP VPN 353
 - L2TP VPN 363
 - PPTP VPN 352
 - RADIUS 483
 - TACAS+ 485
- service group
 - creating 221
 - deleting 222
 - editing 222
- Session Initiation Protocol 198
- Set Date and Time tab 466, 467, 468
- SG565
 - feature only 184
- share
 - network for antivirus 330
- Shares
 - storage 525
- SIP 198
 - UDP port 5060 198
- SIP proxy
 - disabling 199
- SNMP
 - disabling agent 496

- enabling agent 495
- snort command 574
- Snort configuration 294
- soft reboot 511
- source NAT 257
- source NAT rule
 - creating 258
 - deleting 262
 - disabling 261
 - enabling 262
- spanning tree protocol 122
- spool
 - print 534
- sscep utility 575
- SSL
 - Open 420
 - tunnel server 458
- SSL certificate
 - creating 211
 - uploading 210
- static
 - routes 139
- static host
 - creating 160
 - deleting 161
 - editing 161
- static IP address 64
- status
 - refreshing IPSec VPN tunnels 382
- storage
 - network for Web cache 180
 - shares 525
- support
 - technical 26
 - technical report 28
- system log
 - persistent remote 501
 - remote 501
- System tab 497

T

- tab
 - Local Syslog 499
 - Set Date and Time 466, 467, 468
- TACACS+ server 485
- tagged
 - VLAN 129
- TCP 515
 - network port 542

- tcpblast 575
- technical support 26
 - report 28
- test
 - ping 503
 - trace route 504
- Text Save/Restore 474
- TFTP
 - connection tracking 274
 - flash firmware upgrade 516
- ToS traffic shaping 193
- trace route
 - test 504
- traffic
 - shaping 190
- traffic shaping
 - ToS 193
- traversal support
 - NAT 419
- troubleshooting
 - GRE tunnel 138
- TrustedSource 340
 - disabling 345
- tunnel
 - authenticating with preshared secret 369
 - authenticating with x509 certificate 368
 - deleting IPSec VPN 386
 - GRE 136
 - HTTP client 453
 - HTTP server 455
- tunnel server
 - SSL 458
- Type of Service (ToS)
 - traffic shaping 193

U

- UDP port 5060 198
- unblocking
 - URL 308, 310
- Universal Plug and Play gateway 270
- untagged
 - VLAN 129
- upgrading
 - firmware with Netflash 553
 - flash firmware via HTTP 514
 - flash firmware via TFTP 516
- uploading
 - configuration file 521
 - NASL scripts 316

- SSL certificate 210
- Webwasher certificate and private key 321

UPnP

- configuring gateway 270
- configuring rules from Windows XP 272
- refresh view of port forwards 273

URL

- allowing 307
- blocking 308
- blocking Webwasher categories 323
- deleting blocked 308, 310

USB

- detected devices 505
- local storage for antivirus 331
- partitioning storage device 529
- storage 184

user

- adding local 480
- adding PPTP 355
- deleting administrative 478
- deleting local 482
- editing administrative 478
- editing local 482
- root 476

V

viewing

- connection 36
- content filter reporting 324
- firmware version 497
- memory 497
- system uptime 497

Virtual Local Area Network 127

virus

- scanning FTP for 338

VLAN 127

- adding 127
- adding port-based 132
- deleting port-based 135
- editing port-based 134
- enabling port-based 130
- limitations of port-based 130
- tagged 129
- untagged 129

VPN

- disabling IPSec 386
- IPSec 410
- L2TP client 373

- L2TP server 363
- offloading IPsec 444
- PPTP client 349
- PPTP server 352
- VPN server
 - enabling PPTP 353

W

- WDS 113
- Web
 - cache 182
 - configuring management console 208
 - Lists 307
- Web cache 176
 - advanced configuration 187
 - disabling 178
 - enabling 177
 - network storage 180
- Webwasher 319
 - blocking categories 323
 - uploading certificate and private key 321
- Webwasher content filtering
 - disabling 321
- Windows XP
 - configuring UPnP rules 272
- Windows XP client
 - connecting dial-in 69
- wireless
 - configuring advanced 116
 - configuring connection 100
- Wireless Distribution System 113
- WPA2 99

X

- x509 certificate
 - authenticating tunnel 368

Z

- Zebra program 577
- zone
 - demilitarized 94



your **trusted source**
for enterprise security™

Web Gateway – Comprehensive protection against malware, viruses, data leakage and Internet misuse, while ensuring policy enforcement, regulatory compliance, and a productive application environment.

Messaging Gateway – Inbound defense against spam, viruses, denial-of-service and intrusions; outbound protection against data leaks and policy violations.

Network Gateway – World's strongest firewall appliance contains the most comprehensive set of security solutions consolidated in one appliance and automatically discards huge volumes of unwanted traffic from known "bad" entities.

Identity & Access Management – Providing safe access to applications, data, and resources through policy-driven security and strong authentication.

Secure Computing Corporation

www.securecomputing.com

Corporate Headquarters

4810 Harwood Road
San Jose, Ca 95124 USA

Tel +1.800.379.4944
Tel +1.408.979.6100
Fax +1.408.979.6501

European Headquarters

1, The Arena
Downshire Way
Bracknell
Berkshire, RG12 1PU UK

Tel +44.0.870.460.4766
Fax +44.0.870.460.4767

Asia/Pac Headquarters

1604-5 MLC Tower
248 Queen's Road East
Wan Chai, Hong Kong

Tel +852.2520.2422
Fax +852.2587.1333

Japan Headquarters

Level 15 JT Bldg.
2-2-1 Toranomon Minato-Ku
Tokyo 105-0001 Japan

Tel +81.3.5114.8224
Fax +81.3.5114.8226

SECURE COMPUTING®

SnapGear®
Network Gateway Security

For more information, visit us at:

www.securecomputing.com

Trademarks

© 2007 Secure Computing Corporation. All Rights Reserved. Secure Computing, SafeWord, Sidewinder, Sidewinder G2, Sidewinder G2 Firewall, SmartFilter, Type Enforcement, CipherTrust, IronMail, IronIM, SoftToken, Enterprise Strong, Mobile Pass, G2 Firewall, PremierAccess, SecureSupport, SecureOS, Bess, Cyberguard, SnapGear, Total Stream Protection, Webwasher, Strikeback and Web Inspector are trademarks of Secure Computing Corporation, registered in the U.S. Patent and Trademark Office and in other countries. G2 Enterprise Manager, SmartReporter, SecurityReporter, Application Defenses, Central Management Control, RemoteAccess, SecureWire, TrustedSource, On-Box, Securing connections between people, applications and networks and Access Begins with Identity are trademarks of Secure Computing Corporation.